1/2017

Datenschutz Nachrichten

40. Jahrgang
ISSN 0137-7767
12,00 Euro



■ Verbraucherverbandsklage bei Datenschutzverstößen ■ Daten als un/entgeltliche Gegenleistung? ■ Die Einwilligung des Minderjährigen in der DSGVO ■ Einwilligung oder gesetzliche Regelung? ■ Kommentare ■ Stellungnahmen ■ Pressemitteilungen ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechungen ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt

Termine



Montag, 01. Mai 2017
Redaktionsschluss DANA 2/2017
Thema: BDSG-Nachfolgegesetz
alternativ Geheimdienste

Freitag, 05. Mai 2017, 18:00 Uhr
Big Brother Awards
Bielefeld, Hechelei
https://bigbrotherawards.de/

Samstag, 06. Mai 2017
DVD-Vorstandssitzung
Bielefeld. Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

Dienstag, 01. August 2017
Redaktionsschluss DANA 3/2017
Thema: 40 Jahre DVD

Foto: Uwe Schlick / pixelio.de

DANA
Datenschutz Nachrichten
ISSN 0137-7767
40. Jahrgang, Heft 1

Herausgeber
Deutsche Vereinigung für
Datenschutz e.V. (DVD)
DVD-Geschäftstelle:
Reuterstraße 157, 53113 Bonn
Tel. 0228-222498
IBAN: DE94 3705 0198 0019 0021 87
Sparkasse KölnBonn
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Thilo Weichert
c/o Deutsche Vereinigung für
Datenschutz e.V. (DVD)
Reuterstraße 157, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekenn-
zeichneter Artikel verantworten die
jeweiligen Autoren.

Layout und Satz
Frans Jozef Valenta, 53119 Bonn
valenta@datenschutzverein.de

Druck
Onlineprinters GmbH
Rudolf-Diesel-Straße 10
91413 Neustadt a. d. Aisch
www.diedruckerei.de
Tel. +49 (0) 91 61 / 6 20 98 00
Fax +49 (0) 91 61 / 66 29 20

Bezugspreis
Einzelheft 12 Euro. Jahresabonne-
ment 42 Euro (incl. Porto) für vier
Hefte im Kalenderjahr. Für DVD-
Mitglieder ist der Bezug kostenlos.
Das Jahresabonnement kann zum
31. Dezember eines Jahres mit einer
Kündigungsfrist von sechs Wochen
gekündigt werden. Die Kündigung ist
schriftlich an die DVD-Geschäftsstel-
le in Bonn zu richten.

Leserbriefe
Leserbriefe sind erwünscht. Deren
Publikation sowie eventuelle Kür-
zungen bleiben vorbehalten.

Abbildungen, Fotos
Frans Jozef Valenta,
wenn nicht anders gekennzeichnet

Editorial

Der Datenschutz befindet sich in schwerem Gewässer: Konnten wir noch Mitte 2016 über eine fortschrittliche Europäische Datenschutz-Grundverordnung (DSGVO) jubilieren (DANA 2/2016), so brachte die Zeit danach einige politische Dämpfer.

Der erste Dämpfer kam mit den ersten Referententwürfen zum (allgemeinen) Bundesdatenschutzgesetz als Umsetzungsgesetz zur DSGVO. Diese signalisierten, dass die Bundesregierung nicht gewillt ist, im Datenschutz innovative Wege weiterzugehen, sondern dass es das Ziel ist, soweit dies das europäische Recht überhaupt zulässt, den Datenschutz zurückzuschrauben (DANA 4/2016, 180 ff.). Am 1. Februar 2017 krönte die Bundesregierung ihre Bestrebungen mit einem Kabinettsbeschluss, der, sollte dieser so Gesetz werden, die Anwendungspraxis vor neue ungelöste Probleme stellen wird. Es ist offensichtlich, dass für die Bundesregierung eine – unabhängige, aber nicht gerade revolutionär auftretende – Datenschutzaufsicht schon zu viel Kontrollverlust darstellt, weshalb sie diese Aufsicht auszubremsen versucht. Die politischen Initiativen der Bundesregierung – die nun auch im Sicherheitsbereich tiefe Spuren hinterlassen – werden orchestriert von Äußerungen von Regierungsmitgliedern, von Merkel über Gabriel bis zu den Tiefen eines Dobrindt, die entweder von geringer Wertschätzung für digitalen Grundrechtsschutz oder aber von faktischer Ignoranz zeugen (DANA 4/2016, 172). Digitales ist hipp, wenn es Pekuniäres verspricht oder eine Gefahr gewittert wird. Diese Gefahr kann im Terrorismus liegen, oder ganz banal darin, dass das Digitale die eigene Wiederwahl für den Bundestag beeinträchtigen könnte.

Ein größerer politischer Tiefschlag für den Datenschutz könnte noch aus den USA kommen, nachdem der neue US-Präsident erste Signale abgegeben hat, dass er Persönlichkeitsrechte nicht nur verbal gegenüber seinen politischen Gegnern mit Füßen tritt, sondern dass digitaler Grundrechtsschutz auch für seine Politik keine Relevanz hat (die erste Meldung dazu auf S. 55). Darin liegt unzweifelhaft eine große Bedrohung. Möglicherweise verbirgt sich aber dahinter eine Chance, dass in den USA die aufgeklärt, liberal und humanitär gesinnten Menschen einen Aufstand wagen und das Pendel politisch zurückschlagen lassen. Darin liegt auch insofern für den europäischen Datenschutz eine Chance, wenn die Silicon-Valley-Besoffenheit vieler Europäer einer Besinnung auf europäische Werte weicht, zu denen nun unbestreitbar der Datenschutz gehört. Gerade die Wirtschaft müsste angesichts des Trumpschen Handelsprotektionismus die Chance erkennen, mit einem Grundrechts-Protektionismus Geschäfte zu machen.

Das sind aber derzeit noch ungelegte Eier, über deren Ausbrüten wir in der nächsten DANA berichten werden. Die aktuelle Ausgabe befasst sich mit dem Datenschutz als Verbraucherschutz. Vorgestellt werden dabei drei zentrale Themen: die neu eingeführte Verbandsklage (Thilo Weichert), die Nutzung von Personendaten als unerkanntes Entgelt für die Bereitstellung von IT-Services (Tatjana Halm) und die Einwilligung von Minderjährigen (Stefan Ernst). Außerdem erfolgt eine umfassende Bestandsaufnahme des Datenschutzes im Bereich der Doping-Bekämpfung durch Jacob Kornbeck. Bei aller Größe der globalen Herausforderungen ist es eben auch nötig, in den praktischen Anwendungsfeldern des Datenschutzes aktiv zu bleiben.

Thilo Weichert

Autorinnen und Autoren dieser Ausgabe:

Prof. Dr. Stefan Ernst, Rechtsanwalt
info@kanzlei-ernst.de, Freiburg

Tatjana Halm
Referatsleiterin Markt und Recht, Verbraucherzentrale Bayern,
Halm@vzbayern.de, München,

Dr. Jacob Kornbeck
Mitarbeiter verschiedener Gremien in der Europäischen Union,
kornbeck.laskowska@skynet.be, Brüssel

Dr. Thilo Weichert
Vorstandsmitglied der DVD, Netzwerk Datenschutzexpertise,
weichert@datenschutzverein.de, Kiel

Thilo Weichert

Verbraucherverbandsklage bei Datenschutzverstößen

Am 23.02.2016 trat das am 17.12.2015 vom Bundestag verabschiedete Gesetz zur Verbesserung der zivilrechtlichen **Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts** in Kraft. Das Gesetz gibt u. a. Verbraucherschutzorganisationen erstmals explizit das Recht, gegen Datenschutzverstöße zu klagen. Die Regelung, die auch nach dem Wirksamwerden der Europäischen Datenschutzgrundverordnung (DSGVO) Bestand haben wird, wird inzwischen vom Verbraucherzentrale Bundesverband (vzbv) gezielt genutzt, um den Verbraucherdatenschutz bei notorischen Gesetzesverletzern im digitalen Konsumbereich durchzusetzen. Der vorliegende Text stellt die Rahmenbedingungen und die neuen Möglichkeiten beim Verbraucherdatenschutz vor.

1 Ausgangslage

Bis zum Inkrafttreten des neuen Gesetzes waren die Möglichkeiten der Verbandsklage zur Durchsetzung des Datenschutzes begrenzt und stark umstritten. Zwar haben die **Betroffenen** seit jeher das Recht, zivilrechtlich gegen Unternehmen vorzugehen, die ihr Recht auf informationelle Selbstbestimmung verletzen. Geltend gemacht werden können Ansprüche aus den Betroffenenrechten (Benachrichtigung, Auskunft, Berichtigung, Löschung, Sperrung) sowie auf Schadenersatz (§§ 7, 33 ff. BDSG). In der Praxis blieben derartige Gerichtsverfahren aber die große Ausnahme. Der Grund dafür ist, dass die Betroffenen ihr Recht oft nicht kennen, dass die Beeinträchtigung oft nicht und nicht in ihrem Ausmaß erkannt wird bzw. nicht direkt spürbar ist und sich zumeist (nur) im Immateriellen abspielt, und dass der Klageaufwand eines vereinzelten Klägers gewaltig und das Prozessrisiko und die Kosten oft nicht kalkulierbar sind. Zudem entwickelt ein Gerichtsurteil nur Wirkung zwischen den Betroffenen und hindert das Unternehmen bei anderen Kunden nicht an der Fortsetzung unzulässiger Praktiken. Inwieweit darüber hinausgehende Klagemöglichkeiten der Betroffenen bestehen, ist äußerst fraglich. Nach den §§ 1004 analog, 823 BGB ist für Unterlassungs- und Beseitigungsansprüche eine konkrete individuelle Rechtsverletzung und Widerholungsgefahr nötig. Derartiges ist z. B. bei technisch-organisatorischen Verstößen oft nicht nachweisbar.

Den Betroffenen steht zudem die unentgeltliche Möglichkeit der **Anrufung der Datenschutzaufsichtsbehörden** nach § 38 BDSG offen, wovon auch rege Gebrauch gemacht wird. Wegen den begrenzten Ressourcen der Aufsichtsbehörden, für die das Opportunitätsprinzip gilt, dauert die Bearbeitung solcher Beschwerden regelmäßig lange, findet oft keinen oder keinen befriedigenden Abschluss und endete bisher in vielen Fällen nur in einer rechtlich weitgehend folgenlosen Beanstandung.

Verbraucherverbände können **vorgerichtlich** durch öffentliche Aufrufe oder sonstige Öffentlichkeitsarbeit widerrechtliches Verhalten von Unternehmen thematisieren und angreifen.

Anerkannten Verbraucher- und Wirtschaftsverbänden stand außerdem schon bisher nach § 1 UKlaG die Möglichkeit offen, Verbandsklagen gegen **Allgemeine Geschäftsbedingungen** (AGB) zu erheben, auch wenn deren Gegenstand personenbezogene Datenverarbeitung ist. Hiervon machten Verbraucherverbände regen und oft erfolgreichen Gebrauch. Dieses Vorgehen wird dadurch erleichtert, dass AGB zumeist auf den Webseiten der Unternehmen zu finden sind und eine vom Einzelfall losgelöste abstrakte Prüfung möglich ist. Die näheren Umstände der konkreten Datenverarbeitung müssen zumeist nicht festgestellt und analysiert werden.

Verbraucherverbände sind zudem bei **Verstößen gegen das UWG** gem. § 8 Abs. 3 Nr. 3 UWG anspruchsberechtigte Stellen. Durch Verbraucherverbände beklagt werden konnten schon bisher z. B. gemäß § 7 Abs. 2 UWG sog. Cold Calls, bei denen Verbraucherdaten ohne vorherige Einwilligung für werbliche Zwecke genutzt wurden.

Umstritten war bisher, ob und wenn ja welchen **Datenschutzregelungen als Verbraucherschutzgesetze** i. S. v. § 4 Nr. 11 UWG a. F. anzusehen sind, deren Verstoß unlauter ist. Zwar nahm die Zahl der Gerichte, die insofern positiv entschieden, zu, doch weigerte sich insbesondere der Bundesgerichtshof bis zuletzt zu akzeptieren, dass Datenschutzrecht weitgehend Markt- und Verbraucherrelevanz hat.

Auch **Konkurrenten im Wettbewerb** hatten auf der Basis von § 8, 3, 3a, 4 UWG keine weitergehenden Klagemöglichkeiten, da gemäß der lange herrschenden Meinung im Schrifttum und in der Rechtsprechung das BDSG keine Marktverhaltensvorschriften enthielt. Die Schutzziele des Persönlichkeitsschutzes und des Markt- und Verbraucherrechts wurden als zu unterschiedlich angesehen (s. u. 4). Erfolgreiche Klagen von Konkurrenten sind bisher äußerst selten geblieben.

Die nachhaltige Weigerung wesentlicher Teile der Rechtsprechung, Datenschutzregelungen als Marktverhaltensvorschriften anzuerkennen, steht im krassen Widerspruch zu der Erkenntnis, dass viele Firmen im Informations- und Kommunikationssektor, insbesondere US-Unternehmen, Datenschutzverstöße zur Grundlage ihres Geschäftsmodells machten und damit eine **Marktmacht** erlangten, die die analoge Wirtschaft weit hinter sich ließ. Insbesondere das Google-Unternehmen Alphabet mit einer Marktkapitalisierung von 242,5 Mrd. Dollar und Facebook mit einer Kapitalisierung von 304,4 Mrd. Dollar

begründen ihre Dominanz fast vollständig auf dem Angebot personenbezogener Dienstleistungen insbesondere im Internet und der Verwendung der dabei erlangten Daten für Werbezwecke und konnten damit zu den wertvollsten Unternehmen weltweit aufsteigen. Ein Ende des Trends der weiter zunehmenden Kommerzialisierung personenbezogener Daten ist nicht absehbar.

Die Politik in Deutschland und Europa weigerte sich lange, diese Umstände zur Kenntnis zu nehmen, schaute verwundert nach Kalifornien ins Silicon Valley und propagierte für die einheimische Wirtschaft, den dortigen Vorbildern nachzustreben. Erst langsam setzt sich die Erkenntnis bei einigen Politikern durch, dass der wirtschaftliche Erfolg vieler Informationstechnik- (IT-) Unternehmen eine zentrale Grundlage darin findet, dass lokale und europäische **rechtliche Regelungen gebrochen** oder schamlos ausgenutzt werden. Dies gilt nicht nur für den Datenschutz, sondern auch für das Steuerrecht – durch den Einsatz internationaler Steuervermeidungsstrategien – oder für das Kartellrecht – etwa durch den Aufkauf von konkurrierenden oder ergänzenden Start-Ups. Die Einsicht, dass personenbezogene Daten als vermögenswerter Vorteil steuerrechtlich relevant sein könnte und dass eine angebotsübergreifende Nutzung von Personendaten Monopole entstehen lassen kann, hatte bis heute noch keine gesetzgeberischen Konsequenzen. Derweil wird über handelsrechtliche Übereinkommen versucht, sich datenschutzrechtlicher Wettbewerbsbeschränkungen zu entledigen.

Die Wirkung des bisherigen Regelungsrahmens und der unzureichenden Ausstattung der Datenschutzaufsicht ist, dass im Bereich des Datenschutzrechtes allgemein wie auch insbesondere im Bereich des Verbraucherdatenschutzes ein großes **Vollzugsdefizit** besteht, das den Gesetzgeber zum Tätigwerden veranlasste.

2 Die neuen Regelungen

In § 2 Abs. 1 Unterlassungsklagegesetz (UKlaG) wird der Anspruch bei verbraucherschutzgesetzwidrigen Praktiken von einer „Unterlassung" um eine „Beseitigung" erweitert. In Satz 2 des Absatzes heißt es nun:

Werden die Zuwiderhandlungen in einem Unternehmen von einem Mitarbeiter oder Beauftragten begangen, so ist der Unterlassungsanspruch oder der Beseitigungsanspruch auch gegen den Inhaber des Unternehmens begründet. Bei Zuwiderhandlungen gegen die in Absatz 2 Satz 1 Nummer 11 genannten Vorschriften richtet sich der Beseitigungsanspruch nach den entsprechenden datenschutzrechtlichen Vorschriften.

In Abs. 2 wurde eine Nr. 11 eingefügt.

Verbraucherschutzgesetze im Sinne dieser Vorschrift sind insbesondere
11. die Vorschriften, welche die Zulässigkeit regeln
a) der Erhebung personenbezogener Daten eines Verbrauchers durch einen Unternehmer oder
b) der Verarbeitung oder der Nutzung personenbezogener Daten, die über einen Verbraucher erhoben wurden, durch einen Unternehmer, wenn die Daten zu Zwecken der Werbung, der Markt- und Meinungsforschung, des Betreibens einer Auskunftei, des Erstellens von Persönlichkeits- und Nutzungsprofilen, des Adresshandels, des sonstigen Datenhandels oder zu vergleichbaren kommerziellen Zwecken erhoben, verarbeitet oder genutzt werden.

Angefügt wird ein Abs. 2 S. 2:

Eine Datenerhebung, Datenverarbeitung oder Datennutzung zu einem vergleichbaren kommerziellen Zweck im Sinne des Satzes 1 Nummer 11 liegt insbesondere nicht vor, wenn personenbezogene Daten eines Verbrauchers von einem Unternehmer ausschließlich für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Verbraucher erhoben, verarbeitet oder genutzt werden.

Die neue Regelung zu den klageberechtigten Stellen in § 4 – Qualifizierte Einrichtungen – erhält folgende Fassung:

(1) Das Bundesamt für Justiz führt die Liste der qualifizierten Einrichtungen, die es auf seiner Internetseite in der jeweils aktuellen Fassung veröffentlicht und mit Stand 1. Januar eines jeden Jahres im Bundesanzeiger bekannt macht. Es übermittelt die Liste mit Stand zum 1. Januar und zum 1. Juli eines jeden Jahres an die Europäische Kommission unter Hinweis auf Artikel 4 Absatz 2 der Richtlinie 2009/22/EG.
(2) In die Liste werden auf Antrag rechtsfähige Vereine eingetragen, zu deren satzungsmäßigen Aufgaben es gehört, Interessen der Verbraucher durch nicht gewerbsmäßige Aufklärung und Beratung wahrzunehmen, wenn
1. sie mindestens drei Verbände, die im gleichen Aufgabenbereich tätig sind, oder mindestens 75 natürliche Personen als Mitglieder haben,
2. sie mindestens ein Jahr bestanden haben und
3. auf Grund ihrer bisherigen Tätigkeit gesichert erscheint, dass sie ihre satzungsmäßigen Aufgaben auch künftig dauerhaft wirksam und sachgerecht erfüllen werden.
Es wird unwiderleglich vermutet, dass Verbraucherzentralen und andere Verbraucherverbände, die mit öffentlichen Mitteln gefördert werden, diese Voraussetzungen erfüllen. Die Eintragung in die Liste erfolgt unter Angabe von Namen, Anschrift, Registergericht, Registernummer und satzungsmäßigem Zweck. Sie ist mit Wirkung für die Zukunft aufzuheben, wenn
1. der Verband dies beantragt oder
2. die Voraussetzungen für die Eintragung nicht vorlagen oder weggefallen sind.
Ist auf Grund tatsächlicher Anhaltspunkte damit zu rechnen, dass die Eintragung nach Satz 4 zurückzunehmen oder zu widerrufen ist, so soll das Bundesamt für Justiz das Ruhen der Eintragung für einen bestimmten Zeitraum von längstens drei Monaten anordnen. Widerspruch und Anfechtungsklage haben im Fall des Satzes 5 keine aufschiebende Wirkung.
(2a) Qualifizierte Einrichtungen, die Ansprüche nach § 2 Absatz 1 wegen Zuwiderhandlungen gegen Verbraucherschutzgesetze nach § 2 Absatz 2 Satz 1 Nummer 11 durch Abmahnung oder Klage geltend gemacht haben, sind verpflichtet, dem Bundesamt für Justiz jährlich die Anzahl dieser Abmahnungen und erhobenen Klagen mitzuteilen und über die Ergebnisse der Abmah-

nungen und Klagen zu berichten. Das Bundesamt für Justiz berücksichtigt diese Berichte bei der Beurteilung, ob bei der qualifizierten Einrichtung die sachgerechte Aufgabenerfüllung im Sinne des Absatzes 2 Satz 1 Nummer 3 gesichert erscheint.
(3) Entscheidungen über Eintragungen erfolgen durch einen Bescheid, der dem Antragsteller zuzustellen ist. Das Bundesamt für Justiz erteilt den Verbänden auf Antrag eine Bescheinigung über ihre Eintragung in die Liste. Es bescheinigt auf Antrag Dritten, die daran ein rechtliches Interesse haben, dass die Eintragung eines Verbands in die Liste aufgehoben worden ist.
(4) Ergeben sich in einem Rechtsstreit begründete Zweifel an dem Vorliegen der Voraussetzungen nach Absatz 2 bei einer eingetragenen Einrichtung, so kann das Gericht das Bundesamt für Justiz zur Überprüfung der Eintragung auffordern und die Verhandlung bis zu dessen Entscheidung aussetzen.
(5) Das Bundesministerium der Justiz und für Verbraucherschutz wird ermächtigt, durch Rechtsverordnung, die der Zustimmung des Bundesrates nicht bedarf, die Einzelheiten des Eintragungsverfahrens, insbesondere die zur Prüfung der Eintragungsvoraussetzungen erforderlichen Ermittlungen, sowie die Einzelheiten der Führung der Liste zu regeln.

Eingefügt wurde weiterhin ein § 12a – Anhörung der Datenschutzbehörden in Verfahren über Ansprüche nach § 2:

Das Gericht hat vor einer Entscheidung in einem Verfahren über einen Anspruch nach § 2, das eine Zuwiderhandlung gegen ein Verbraucherschutzgesetz nach § 2 Absatz 2 Satz 1 Nummer 11 zum Gegenstand hat, die zuständige inländische Datenschutzbehörde zu hören. Satz 1 ist nicht anzuwenden, wenn über einen Antrag auf Erlass einer einstweiligen Verfügung ohne mündliche Verhandlung entschieden wird.

3 Auslegung der Regelungen

Im Folgenden sollen Hinweise für die Auslegung der neuen Regelungen gegeben werden.

3.1 Erfasste Vorschriften und Zweckrichtung

§ 2 Abs. 2 S. 1 Nr. 11 UKlaG zählt die Vorschriften nicht ausdrücklich auf, deren Verstoß eine Verbandsklage ermöglicht. Mit der dynamischen Norm werden **alle in Deutschland geltenden datenschutzrechtlichen Regelungen**, also insbesondere das BDSG, sonstige Landes- und Bundesgesetze sowie umsetzende Rechtsverordnungen, und künftig auch die DSGVO, erfasst. Verstöße gegen unternehmensinterne Regelungen können nicht geltend gemacht werden, möglicherweise aber solche gegen genehmigte Verhaltensregeln nach § 38a BDSG (Art. 40, 41 DSGVO), soweit diese allgemeine Gesetzesnormen konkretisieren.

Die Regelung erstreckt die Verbandsklagebefugnis auf Vorgänge, bei denen es um Werbung, Markt- und Meinungsforschung, das Betreiben einer Auskunftei, das Erstellen von Persönlichkeits- und Nutzungsprofilen (vgl. § 15 Abs. 3 S. 1 TMG), Adresshandel, sonstigen Datenhandel oder vergleichbare kommerzielle Zwecke geht. Erfasst wird damit die Erhebung von Verbraucherdaten mit Hilfe von Cookies sowie anderen Identifikatoren zum Zweck der Profilbildung, der Werbung oder des Datenverkaufs. Persönlichkeitsprofile werden dann erstellt, wenn personenbeziehbare Daten einer Person zusammengeführt und systematisch verknüpft werden, um durch analytische Auswertungen neue Erkenntnisse über die Betroffenen, etwa zur Bonität oder zum Bewegungsverhalten, zu finden. Die scheinbare normative Begrenzung erfasst tatsächlich den gesamten „Verbraucherdatenschutz“, da als gemeinsame äußere Klammer die „**kommerziellen Zwecke**“ genannt werden. Auf die Erkennbarkeit der Verbrauchereigenschaft für die Unternehmen kommt es ebenso wenig an wie bei der Anwendung anderer Verbraucherschutzvorschriften.

Keine kommerziellen Zwecke werden verfolgt, wenn ein Unternehmen Verbraucherdaten ausschließlich **zur Erfüllung gesetzlicher Pflichten** verarbeitet. Die Begründung erwähnt insofern die §§ 10, 25 KWG. Entsprechendes gilt z. B. für die Datenspeicherung nach § 147 AO oder nach dem GwG. Werden die derart erfassten Daten darüber hinausgehend aber auch für kommerzielle Zwecke – also im Verhältnis zum Verbraucher – verwendet, so ist insofern die Verbandsklage möglich.

Nicht erfasst sind der Arbeitnehmerdatenschutz oder der sog. B2B-Bereich, da dann „**Verbraucher**“ nicht betroffen sind. Verbraucher ist gemäß § 13 BGB jede natürliche Person, die ein Rechtsgeschäft abschließt, das überwiegend weder ihrer gewerblichen noch ihrer selbständigen beruflichen Tätigkeit zugerechnet werden kann. Erfasst wird schon die Suche im Internet, nicht nur zur Vorbereitung eines Rechtsgeschäftes, wenn die erhobenen Daten für Werbezwecke weiterverwendet werden. Es bedarf dabei nicht der Anbahnung eines konkreten Geschäftsabschlusses oder eines ähnlichen geschäftlichen Kontaktes gemäß § 311 BGB.

Kontrovers diskutiert wird die Frage, inwieweit rechtlich geforderte **technisch-organisatorische Maßnahmen** (§ 9 BDSG, Art. 25, 32 DSGVO) zum Gegenstand einer Verbandsklage gemacht werden können. Dies wird weitgehend mit dem Hinweis auf die Zweckbeschränkung in Nr. 11 abgelehnt. Diese Argumentation greift aber nicht, soweit bei den Maßnahmen Verbraucherdaten betroffen sind. In diesen Fällen werden kommerzielle Zwecke verfolgt; der Zweck der Datensicherheit kann hiervon nicht getrennt werden. In der Praxis erwiesen sich Sicherheitsdefizite und daraus resultierende Datenlecks immer wieder als besonders verbraucherschädigend, etwa wenn durch unzureichende Datensicherheit Nutzungsdaten Unberechtigten zur Kenntnis kamen. Ein Schaden für den Verbraucher kann sowohl dadurch entstehen, dass derartige Informationen, etwa kompromittierende wie z. B. Sexbilder, veröffentlicht werden oder wenn die erlangten Daten für Identitätsdiebstahl und den Missbrauch von Accounts verwendet werden.

Rein technische oder organisatorische Mängel **ohne direkten Bezug zur Verbraucherdatenverarbeitung**, die keine Auswirkung auf die Rechtmäßigkeit der Verarbeitung haben, etwa Verstöße bei der Bestellung des betrieblichen Datenschutzbeauftragten, werden nicht erfasst. Hat ein Vorgang nur teilweise einen Verbraucherbezug, so kann auch

nur insofern eine Prüfung durch einen Verband erfolgen.

Nicht erfasst werden vom kollektiven Verbandsklagerecht die individuellen **Betroffenenrechte**, also die Rechte auf Benachrichtigung, Auskunft, Löschung und Sperrung (§§ 33-35, 42a BDSG). Etwas anderes kann aber dann gelten, wenn ein Unternehmen seine Geschäftspraxis so gestaltet, dass generell und systematisch die Betroffenenrechte verletzt werden und dadurch Einfluss auf die Wahrnehmung der Verbraucherrechte generell sowie auf den Wettbewerb genommen wird.

Unter Verweis auf § 2 Abs. 2 S. 2 UKlaG wird dargelegt, kommerzielle Zwecke würden nicht verfolgt, „wenn es um die Begründung, Durchführung oder Beendigung **eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses** mit dem Verbraucher“ gehe. Erfasst sein sollten nur Praktiken, bei denen personenbezogene Daten rechtswidrig zur Handelsware gemacht werden. Tatsächlich ist diese explizite gesetzliche Einschränkung irritierend. Damit wird zum Ausdruck gebracht, dass ein Verbraucherverband nicht in die individualrechtliche Beziehung Unternehmen-Verbraucher eingreifen soll. In der Praxis dürfte dieser Einschränkung aber keine Relevanz zukommen: Ausgenommen sein können nur zulässige Vertragsbeziehungen, bei denen letztlich ohnehin kein Unterlassungs- und Beseitigungsanspruch besteht. Erfasst werden aber Verbrauchervertragsbeziehungen, bei denen es zu einer unzulässigen Datenverarbeitung kommt. Insofern besteht ein besonders hoher Schutzbedarf der Verbraucher. Der klassische Fall der Verbrauchervertragsbeziehung ist, dass die Verbraucher (auch) mit ihren Daten bezahlen. Derartige Konstellationen liegen im Hauptfokus der Neuregelung.

Die Verbandsklage ist beschränkt auf die kommerzielle Datennutzung durch **Unternehmen** (§ 14 BGB). Nicht erfasst werden also Privatpersonen, die gelegentlich Waren oder Dienstleistungen anbieten. Nicht erfasst sein sollen auch Non-Profit-Organisationen und öffentliche Körperschaften. Dies kann aber nur zutreffen, soweit diese nicht kommerziell tätig werden. Kommerziell tätig sind nicht nur Unternehmen, deren Datenverarbeitung Bestandteil des Geschäftsmodell sind, sondern auch solche, bei denen gelegentlich und zwangsläufig Kundendaten erfasst und verarbeitet werden, also z. B. auch Ärzte oder Rechtsanwälte.

Die per Klage zu rügende Handlung muss **Kollektivinteressen von Verbrauchern** berühren. Dies schließt nicht aus, dass es sich hierbei zunächst nur um Einzelfälle handelt, wenn diese Hinweise auf ein systematisches Vorgehen geben und wenn dem Verbraucherverband eine generelle Klärung nötig erscheint. Unzulässig ist es, ausschließlich in Einzelfällen den Ersatz von Aufwendungen und Kosten anzustreben (§ 8 Abs. 4 UWG).

Eine oben nicht abgedruckte gesetzliche Ergänzung der Neuregelung besteht im Zusammenhang mit dem vom Europäischen Gerichtshof für ungültig erklärten **Safe-Harbor-Rechtsrahmen**. Nach § 17 UKlaG findet § 2 Abs. 1 S. 1 Nr. 11 UKlaG keine Anwendung auf Zuwiderhandlungen gegen § 4b BDSG (unzulässige Auslandsdatenübermittlung), wenn diese bis zum 30.09.2016 begangen wird. Hiermit wurde – unnötigerweise – Unternehmen ein verlängerter Vertrauensschutz in Safe Harbor gewährt.

3.2 Aktivlegitimation – Verfahrensfragen

Die Klageberechtigung ergibt sich aus § 3 UKlaG. Die Gesetzesnovelle wurde zum Anlass genommen, eine Anpassung an die Verbandsklagebefugnis nach § 8 Abs. 3 UWG vorzunehmen. Nach dem UKlaG klagebefugt sind also auch Organisationen der Wirtschaft zur Bekämpfung unlauteren Wettbewerbs sowie **Industrie- und Handelskammern** und Handwerkskammern.

§ 4 UKlaG regelt im Detail, welche Organisationen als **qualifizierte Einrichtungen** anzusehen sind und deshalb klageberechtigt sind. Das Bundesamt für Justiz führt eine Liste der qualifizierten Einrichtungen, die auch im Internet abrufbar ist. Der Zweck der Regelung ist auch, rechtsmissbräuchliche Abmahnungen und Klagen durch sog. Abmahnvereine zu verhindern. Vor diesem Hintergrund werden die qualifizierten Einrichtungen verpflichtet, dem Bundesamt für Justiz jährlich einen Bericht über die Anzahl der nach § 2 Abs. 2 S. 1 Nr. 11 UKlaG erhobenen Abmahnungen sowie die „Ergebnisse“ anzuliefern. Von dieser Regelung nicht betroffen sind die Verbraucherzentralen, bei denen die Eignung zur Verbandsklage nach § 4 Abs. 2 S. 2 UKlaG unwiderleglich vermutet wird.

§ 12a UKlaG sieht vor, dass vom Gericht die zuständige inländische **Datenschutzaufsichtsbehörde angehört** wird. Die Regelung ist § 8 Abs. 2 UKlaG nachgebildet, der bei der gerichtlichen Überprüfung von AGB nach § 1 UKlaG unter bestimmten Voraussetzungen eine Anhörung der Bundesanstalt für Finanzdienstleistungsaufsicht vorsieht. Die Anhörungspflicht gilt auch für Verfahren des einstweiligen Rechtsschutzes, es sei denn, dass ohne mündliche Verhandlung entschieden wird (§ 12a S. 2 UKlaG). Wird gegen einen Beschluss Widerspruch eingelegt, ist die Anhörung nachzuholen. Angehört wird nur die inländische örtlich zuständige Aufsicht; eine solche kann es auch geben, wenn die Hauptniederlassung eines Unternehmens im Ausland sitzt. Ob eine und wenn ja welche Stellungnahme abgegeben wird, liegt voll im Entscheidungsbereich der unabhängigen Datenschutzaufsicht. Damit sollen unterschiedliche Voten von Gericht und Aufsichtsbehörde wegen unzureichender Information über den Sachverhalt und die rechtliche Bewertung vermieden werden. Damit ist aber nicht ausgeschlossen, dass das Gericht zu einem von der Aufsichtsbehörde abweichenden Ergebnis kommt. Einbezogen werden dürfen alle relevanten Erkenntnisse der Aufsichtsbehörde. Diese hat insofern eine Befugnis zur Datenweitergabe nach § 38 Abs. 1 S. 3 BDSG. Das gerichtliche und ein möglicherweise laufendes aufsichtliches Verfahren sind aber ansonsten völlig unabhängig. Die anhängige Klage hindert die Aufsichtsbehörde nicht, im Rahmen ihrer Befugnisse selbst tätig zu werden. Das Verbandsklageverfahren kann sogar Auslöser für das aufsichtliche Tätigwerden sein. Die Aufsichtsbehörde ist im Rahmen der Anhörung nicht Verfahrensbeteiligte.

Die Anhörungspflicht verletzt nicht das Gebot der **prozessualen Waffengleichheit** der Parteien. Die Aufsichts-

behörde ist kein Streithelfer, sondern faktisch wie rechtlich der Objektivität gegenüber beiden Parteien verpflichtet. Versteht man sie als Partei, so ist sie allenfalls Partei für den Schutz informationeller Selbstbestimmung; ihre Aufgabe ist es gemäß § 12a UKlaG, die gerichtliche Entscheidungsfindung in dem rechtlich wie technisch oft komplexen Bereich zu erleichtern, nicht zu lenken. Hintergrund der Einbeziehung der Aufsichtsbehörde ist zudem, dass bei den Verfahren regelmäßig ungleiche Parteien gegenüberstehen, wobei das Unternehmen zunächst faktisch die Verarbeitung bestimmen kann. In derartigen Fällen ist der Staat nicht nur berechtigt, sondern verpflichtet, im Rahmen privatrechtlicher Regelungen die Voraussetzungen zu schaffen, dass das Recht auf informationelle Selbstbestimmung als Norm des objektiven Rechts Geltung erlangt.

3.3 Unterlassungs- und Beseitigungsanspruch

Nach § 8 Abs. 1 UWG besteht schon bisher neben dem Unterlassungs- auch ein **Beseitigungsanspruch**. Anderes galt für den bisherigen § 2 UKlaG a. F., der seit der Novellierung nun auch einen Beseitigungsanspruch vorsieht. Wurden unzulässig Daten erhoben und gespeichert, so ergibt sich aus § 2 UKlaG, dass diese auch zu löschen bzw. zu sperren sind (vgl. § 35 BDSG, § 13 Abs. 4 S. 1 Nr. 2, S. 2 TMG). Der Anspruch des klagenden Verbands hat also denselben Inhalt wie der des einzelnen Verbrauchers, beschränkt sich aber nicht darauf. Die § 1004 BGB und § 8 UWG können mit herangezogen werden zur Beseitigung einer rechtswidrigen fortdauernden Störung.

Ist das Unternehmen der Ansicht, dass der kollektivrechtlich geltend gemachte Beseitigungsanspruch den Interessen seiner Kunden widerspricht, so kann es darauf hinwirken, dass die Unzulässigkeit der Datenverarbeitung dadurch beseitigt wird, dass z. B. wirksame Einwilligungen der Betroffenen eingeholt werden. Ein **Interessenkonflikt zwischen Individuum und Kollektiv** kann auch unabhängig von der Unternehmensansicht bestehen, etwa bei einem kollektivrechtlich begründeten Löschungsanspruch und einem individualrechtlichen Beweissicherungsinteresse z. B. zur Durchsetzung von Schadenersatzansprüchen. Das Datenschutzrecht liefert den Regelungsrahmen für die Lösung dieses Konflikts: Besteht Grund zu der Annahme, dass durch eine Löschung schutzwürdige Interessen von Betroffenen beeinträchtigt würden, so tritt an die Stelle einer Löschung die Sperrung (§ 35 Abs. 3 Nr. 2 BDSG). Entsprechendes gilt, wenn ein parallel laufendes aufsichtliches Kontrollverfahren stattfindet und hierfür die eigentlich zu löschenden Daten benötigt werden.

Eine **rechtswidrige Störung** kann darin bestehen, dass ein Unternehmen seine Verbraucher ungenügend über ihre Rechte informiert. Die Beseitigung von Störungen kann auch darauf abzielen, ein Beschwerdemanagementsystem zur Abwicklung konkreter Rechtsverstöße einzurichten oder rechtswidrig vereinnahmte Beträge an die betroffenen Kunden zurückzuzahlen.

Bestehen für eine Störungsbeseitigung **verschiedene Handlungsmöglichkeiten**, so ist dem Schuldner die Wahl des Mittels zu überlassen. Der Anspruch hat sich dann auf die Benennung des Ziels zu beschränken, die aber so präzise wie möglich sein sollte.

Ist eine **unzulässige Datenübermittlung** Gegenstand einer erfolgreichen Verbandsklage, so kann gegenüber dem Datenempfänger die Löschung, Sperrung oder Berichtigung nicht direkt durchgesetzt werden. Wohl aber besteht ein Anspruch auf Benachrichtigung des Empfängers (vgl. § 35 Abs. 7 BDSG).

Ein Manko wird darin gesehen, dass der Beseitigungsanspruch sich nicht ausdrücklich auf § 1 UKlaG und damit auf **AGB** erstreckt.

Nicht eindeutig ist, wie weit die Rechtswirkung einer durch einen Verband erstrittenen Entscheidung geht. Gemäß § 11 UKlaG können sich Verbraucher auf ein auf § 1 UKlaG beruhendes Unterlassungsgebot in Bezug auf AGB in eigener Sache berufen. Ein Verweis auf § 2 Abs. 2 Nr. 11 UKlaG erfolgt in § 11 aber nicht, so dass für **Folgeklagen durch Betroffene** ein erhöhtes Prozessrisiko bestehen bleibt.

3.4 Verhältnis zum UWG

Schon bisher wurden bestimmte datenschutzrechtliche Vorschriften zugleich als verbraucherrelevant und als Marktverhaltensregelungen i. S. v. § 3a UWG angesehen. Der Unterlassungsanspruch gemäß § 8 Abs. 1 UWG kann gemäß § 8 Abs. 3 UWG von Wirtschaftsverbänden, Industrie- und Handelskammern, Handwerkskammern und auch von Verbraucherschutzverbänden geltend gemacht werden. § 2 Abs. 2 S. 1 Nr. 11 UKlaG ist ein weiterer Hinweis darauf, dass Datenschutzvorschriften auch Marktverhaltensvorschriften sind. Hierauf kommt es aber in Zukunft nicht an, da das UKlaG eine eigenständige Klagebefugnis begründet.

3.5 Europäisches Recht

Im Laufe der Gesetzgebung wurde teilweise vorgebracht, das geplante Klagerecht für Verbraucherverbände verstieße gegen europäisches Recht. Art. 28 der **Datenschutzrichtlinie** 95/46 EG (EG-DSRl) sei bzgl. des Vollzugs des Datenschutzrechts abschließend und schlösse daher zusätzliche Durchsetzungsinstrumente aus. Diese Meinung war schon damals falsch, da die Rechtsprechung zur verbindlichen Harmonisierung sich auf materiell-rechtliche abschließende Regelungen beschränkte und sich nicht auf Rechtsschutzmöglichkeiten bezog.

Gemäß Art. 80 Abs. 2 **DSGVO** können nun Mitgliedstaaten vorsehen, dass „eine Einrichtung, Organisation oder Vereinigung ohne Gewinnerzielungsabsicht, die ordnungsgemäß nach dem Recht eines Mitgliedsstaats gegründet ist, deren satzungsmäßige Ziele im öffentlichen Interesse liegen und die im Bereich des Schutzes der Rechte und Freiheiten von Betroffenen Personen in Bezug auf den Schutz ihrer personenbezogenen Daten tätig ist“, unabhängig von einem Auftrag der betroffenen Person in diesem Mitgliedstaat das Recht hat, bei der „zuständigen Aufsichtsbehörde eine Beschwerde einzulegen und die in den Artikeln 78 und 79 aufgeführten Rechte in Anspruch zu nehmen, wenn ihres Erachtens die Rechte einer betroffenen Person gemäß dieser Verordnung infolge einer Verarbeitung verletzt worden sind“. Damit wird klargestellt, dass das deutsche Verbandsklagerecht bei Datenschutzverstößen in Einklang mit europäischem Recht steht.

4 Bewertung

Im Rahmen des Gesetzgebungsverfahrens hatten sich viele Verbändevertreter gegen die Einführung der Verbandsklage im Datenschutzrecht eingesetzt. So wurde von einigen Datenschutzbehörden und u. a. auch von der Deutschen Gesellschaft für Rechtsinformatik (DGRI) vorgebracht, es bedürfte keines neuen verbraucherrechtlichen Instrumentariums; die **bisherigen Instrumente** würde genügen. Soweit dieses Argument von verantwortlichen Stellen vorgetragen wurde, ist deren Motivation offensichtlich: Die Gefahr, dass illegale Geschäftsmodelle angegriffen werden, ist mit dem Gesetz gestiegen.

Soweit die **Aufsichtsbehörden** dieses Argument vortrugen, lag dem die unbegründete Befürchtung zugrunde, Verbraucherorganisationen könnten zur Datenschutzaufsicht in Konkurrenz treten. Tatsächlich ergänzen sich die Kontrollinstrumente im Interesse der Verhinderung von Rechtsverstößen. Zudem hat das Gesetz in § 12a UKlaG eine Verzahnung vorgesehen. Viele Aufsichtsbehörden arbeiten schon effektiv zusammen, ohne dass dies die jeweilige Unabhängigkeit beeinträchtigt. Die Interessenlagen sind weitgehend identisch. Unbestreitbar ist, dass sowohl die bisherige Ausstattung wie auch die bisherigen Sanktionsmöglichkeiten der Aufsichtsbehörden völlig unzureichend waren, was zu einem gewaltigen Vollzugsdefizit beim Datenschutz geführt hat (s. o. 1). Auch wenn sich dies möglicherweise mit Inkrafttreten der DSGVO teilweise ändern wird, so sind wir weiterhin weit von rechtskonformen Zuständen entfernt. Schon in der Vergangenheit hat sich gezeigt, dass sich der zivilgerichtliche Weg von Verbraucherorganisationen zur Durchsetzung des Datenschutzes als erheblich effektiver erwies als der verwaltungsrechtliche oder sanktionsrechtliche der Aufsichtsbehörden, insbesondere wenn es um flächendeckende Datenschutzverstöße großer IT-Unternehmen wie z. B. Facebook, WhatsApp, Google usw. ging. Es ist leider nicht von der Hand zu weisen, dass das Handeln der unabhängigen Datenschutzaufsicht in Einzelfällen von sachfremden Erwägungen getrieben wird, etwa dem Schutz örtlicher Unternehmen. Hierfür gab die Praxis des irischen Datenschutzbeauftragten, der Irland für US-amerikanische IT-Unternehmen zum idealen Standort machte, den beredtsten Beleg. Es gibt Hinweise darauf, dass ein entsprechendes Denken in dem einen oder anderen Fall auch deutsche Aufsichtsbehörden leitet.

Arbeitsteilung und Kooperationen zwischen Verbraucherverbänden und Aufsichtsbehörden können darin bestehen, dass konkrete Ermittlungen von Aufsichtsbehörden durchgeführt werden. Durch die bestehenden Untersuchungsbefugnisse können technische-organisatorische wie auch materiell-rechtliche Feststellungen gemacht werden, die den Betroffenen oder evtl. auch – wenn keine entgegenstehenden Rechte verletzt werden – direkt den Verbraucherverbänden zur Kenntnis gegeben werden können. Verbraucherverbände haben insofern zumeist nur **begrenzte Erkenntnismöglichkeiten**, die sich auf die Oberfläche verbraucherbezogener Datenverarbeitung beschränken. Darin liegt kein unfaires Verfahren, sondern dies basiert auf dem teilweise sich überschneidenden Interesse an der Umsetzung des Datenschutzrechtes. Unternehmen können kein berechtigtes Interesse geltend machen, dass Datenschutzverstöße andauern. Ansätze für Verbraucherklagen können sich auch durch journalistische Recherchen oder durch Informationen von Whistleblowern ergeben.

Die Möglichkeit **divergierender Entscheidungen** zwischen Verbraucherorganisationen und Aufsichtsbehörden, Zivil- und Verwaltungsgerichten ist keine Gefahr, sondern eine Chance, die in einer gewaltengeteilten pluralen Gesellschaft in vielen Bereichen besteht. Sie liegt darin, dass sich die besseren Argumente durchsetzen, nicht der ökonomische oder politische Einfluss, auch nicht eine Ansicht einer zuständigen Instanz. Diese Divergenzen können letztlich höchstrichterlich beseitigt werden. Das Risiko der Verletzung digitaler Grundrechte ist derzeit erheblich höher als das Risiko eines Unternehmens, einer falschen Autorität zu vertrauen. Mit den bestehenden Abstimmungsmechanismen in § 38 Abs. 1 S. 3, 4 BDSG und nun in § 12a UKlaG wie auch künftig in Art. 31 und 60 ff. DSGVO wird das Unternehmensrisiko abweichender Meinungen so weit wie möglich reduziert.

Die lange Zeit propagierte Ansicht, dass **Persönlichkeitsschutz und Verbraucherschutz** zwei systemverschiedene Aufgaben seien, hat keinen realen Hintergrund. Verbraucherschutz ist in Art. 38 GRCh als „softes“ Grundrecht ausgestaltet. Die Rechtsprechung sowohl des EuGH wie des BVerfG lässt unzweifelhaft erkennen, dass die Verteidigung der Grundrechte von Verbrauchern insbesondere in einer Informationsgesellschaft gegenüber mächtigen Unternehmen zu einer wichtigen staatlichen Aufgabe geworden ist. Betroffen von datenschutzwidrigem Marktverhalten sind nicht nur Einzelpersonen, sondern die Verbraucher insgesamt.

5 Praktisches Vorgehen

Erhält eine Verbraucherschutzorganisation von einem Datenschutzverstoß Kenntnis, so weist sie das verantwortliche Unternehmen auf das unzulässige Handeln hin und fordert es auf, das beanstandete Verhalten nicht mehr zu praktizieren und diesbezügliche eine **Unterlassungserklärung** abzugeben. Deren Wirksamkeit setzt voraus, dass für den Fall der Zuwiderhandlung das Versprechen einer Strafzahlung in empfindlicher Höhe abgegeben wird. Wird die Abmahnung nicht akzeptiert, so kann der Anspruch im Regelfall im Wege der einstweiligen Verfügung kurzfristig durchgesetzt werden. Der Abgemahnte hat die Kosten der Abmahnung zu erstatten.

Ein Unterlassungsanspruch kann **auch ohne eine vorangegangene Abmahnung** gerichtlich geltend gemacht werden. In diesem Fall besteht aber das Risiko, dass der Beklagte den Anspruch sofort anerkennt, so dass der Kläger gemäß § 93 ZPO die Prozesskosten tragen muss.

In der Gesetzesbegründung zur aktuellen Rechtsänderung wird darauf hingewiesen, dass das neue Recht der Behebung von Rechtsverstößen dient, nicht der Gewinnerzielung abmahnberechtigter Stellen. Daher sollte insbesondere bei Verstößen kleinerer Unternehmen (z. B. Start-ups) ein **kostenloser Hinweis** mit einer Stellungnahmefrist einer Abmahnung vorausgehen. Ein solches entgegenkommendes Vorgehen darf aber nicht dazu führen, dass Verbraucherverbände nun die Funktion einer unentgelt-

lichen beratenden Rechtsabteilung für kleinere Unternehmen übernehmen.

6. Schlussfolgerungen

Das neue Verbandsklagerecht hat bisher nicht zu einer neuen Klagewelle beim Datenschutz geführt und wird dies auch nicht tun. Dem stehen schon die allzu beschränkten Ressourcen der Verbraucherverbände entgegen. Wohl aber besteht ein Instrument zur objektiven Rechtskontrolle, mit dem bisherige Vollzugsdefizite behoben werden können. Wegen der Prozessunlust von Betroffenen und Aufsichtsbehörden besteht beim Datenschutz ein **Rechtsprechungsdefizit**, das mit dem neuen Instrument reduziert werden kann. Die Verbraucherverbände nehmen dieses gezielt in Anspruch, um insbesondere bei gravierenden und massenhaften Rechtsverletzungen Abhilfe zu schaffen, etwa beim drohenden Datenaustausch zwischen Facebook und WhatsApp.

Durch die Einführung des Verbandsklagerechts hat der deutsche Gesetzgeber die richtige Konsequenz aus dem Umstand gezogen, dass Datenschutz nicht nur der Wahrung individueller, sondern auch kollektiver Schutzgüter dient. Zwar enthält die DSGVO keine entsprechenden Regelungen, ermöglicht aber in Art. 80 den Mitgliedstaaten, hieraus prozessuale Konsequenzen zu ziehen. Neben dem Verbraucherschutz wäre insofern eine **Kollektivklagebefugnis** im Bereich des Beschäftigtendatenschutzes naheliegend, da insofern eine vergleichbare kollektive Interessenlage besteht.

Tatjana Halm

Daten als un/entgeltliche Gegenleistung?

1. Hintergrund

„Man zahlt mit seinen Daten“ – regelmäßig ist dieser Satz im Zusammenhang mit der Nutzung vermeintlich kostenloser Dienstleistungen zu hören. Soziale Netzwerke, Kundenkarten, Apps gehören zu diesen Angeboten, die der Verbraucher auf den ersten Blick scheinbar umsonst nutzen kann.

Dem ist selbstverständlich nicht so und dies ist auch nachvollziehbar. Die Anbieter dieser Dienstleistungen haben – wie jeder andere Anbieter auch – Kosten, die sie begleichen müssen. Personal, Mieten, Arbeitsausstattungen und Vieles mehr wollen erwirtschaftet werden. Es ist ihnen daher gar nicht möglich, ihre Leistung kostenlos anzubieten. Das erforderliche Geld zahlt allerdings *nicht unmittelbar* der Nutzer. Und hier erschließt sich nun der Sinn des einleitenden Satzes, denn der Nutzer zahlt das Geld *mittelbar*, indem seine zur Verfügung gestellten Daten zu Geld gemacht werden. Wie auch immer sich die jeweiligen Geschäftsmodelle ausgestalten. Die wirtschaftliche Bedeutung von Daten ist somit enorm.[1] Big Data wird inzwischen in allen Bereichen genutzt und die diesbezügliche Entwicklung schreitet immer schneller voran. Die Verbraucher allerdings verfügen selbst nur selten über den Wert ihrer Daten.[2] Wie selbstverständlich werden ihre Daten genutzt. Kaum wird noch unterschieden, ob das jeweilige Datum für die Vertragserfüllung erforderlich ist oder ob es sich quasi um eine darüber hinausgehende Gegenleistung handelt.

Die Zurverfügungstellung seiner Daten ist also der Preis, den der Verbraucher für die Nutzung der jeweiligen Dienstleistung zahlt. Aber wenn schlussendlich doch ein Preis gezahlt wird, stellt sich zum einen die Frage, ob dann nicht entsprechende rechtliche Regeln auf die Gestaltung solcher Nutzungsverträge Anwendung finden sollten. Und zudem ist zu fragen, wie sich die immer größere Verlagerung des Datenschutzes in den zivilrechtlichen Bereich auf dessen Ausgestaltung insgesamt auswirkt.

In der Konsequenz ist zu überlegen, ob neben einem **Datenschutzrecht** nicht längst ein **Datenschuldrecht** angezeigt wäre, damit die Datenpreisgabe auch rechtlich als Währungstyp[3] oder kaufähnliche Gegenleistung anerkannt wird. Diese Fragen sollten geklärt werden, um dem Eingangssatz eine Bedeutung zu Teil kommen zu lassen und ihn nicht nur als rechtfertigende Floskel zu erhalten.

2. Status Quo: Daten als entgeltliche Gegenleistung in gesetzlichen Vorschriften?

Im Folgenden wird also die aktuelle Rechtslage im Hinblick auf die Bewertung von Daten als entgeltliche Gegenleistung erörtert.

a. Europarechtliche Regelungen

Die Entwicklung in der europäischen Gesetzgebung lässt eine Tendenz dahin erkennen, die Hingabe von Daten ausdrücklich als Gegenleistung im Vertragsverhältnis anzuerkennen.

- **Verbraucherrechterichtlinie 2011/83/EU (VRRL)**

Bereits der VRRL lassen sich Aussagen zur Datenpreisgabe entnehmen. Uneinigkeit besteht zwar zunächst darüber, ob die VRRL sowohl entgeltliche als auch unentgeltliche Gegenleistungen erfasst. Letzteres hätte zur Folge, dass die hier behandelten Nutzungsverträge nach den Regelungen der VRRL unproblematisch zu bewerten wären, da es auf die Wertung der Datenpreisgabe als Entgelt nicht ankäme.

Dem Wortlaut der Art. 2 Nr. 5 und Nr. 6 VRRL nach heißt es hinsichtlich

Verbraucherverträgen: „*und der Verbraucher hierfür einen* ***Preis*** *zahlt*“. Nach Auffassung des deutschen Gesetzgebers allerdings erfasst die VRRL daher nur Verträge, bei denen die Waren oder Dienstleistungen **gegen Entgelt** erbracht werden, also entgeltliche Verträge.[4] Dies hat sich ungeachtet anderer Ansichten bei der Umsetzung in die deutsche Gesetzgebung so durchgesetzt.

Jedoch ist weiter zu fragen, wie sich das Erfordernis des zu zahlenden Preises dabei bestimmt. Dieses ist weit auszulegen. Daher können auch Verträge, bei denen der Verbraucher für die Erbringung einer Dienstleistung oder die Lieferung einer Ware dem Unternehmer im Gegenzug personenbezogene Daten mitteilt und in deren Speicherung, Nutzung oder Weitergabe einwilligt, erfasst sein.[5] Letztendlich ergibt sich daraus, dass die Mitteilung personenbezogener Daten durchaus als „Preis“ im Sinne der VRRL zu sehen ist und somit als entgeltlicher Vertrag zu werten ist. Auf den Streit, ob auch unentgeltliche Gegenleistungen von der VRRL erfasst sind, käme es somit nicht an.

- **Richtlinienvorschlag über vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte (DIRL)**

Der zeitlich neuere Richtlinienvorschlag über vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte (DIRL) positioniert sich hier ähnlich.[6] Gemäß Art. 2 Nr. 6 DIRL ist unter „Preis“ im Sinne des Richtlinienvorschlages zwar noch „***Geld****, das im Austausch für bereitgestellte digitale Inhalte geschuldet ist*“ zu verstehen.

Der Anwendungsbereich der RL erstreckt sich nach Art. 3 Abs. 1 DIRL auf alle Verträge, auf deren Grundlage ein Anbieter einem Verbraucher digitale Inhalte bereitstellt oder sich hierzu verpflichtet und der Verbraucher als Gegenleistung einen Preis zahlt oder **aktiv eine andere Gegenleistung als Geld** in Form personenbezogener oder anderer Daten erbringt. Art. 3 Abs. 1 DIRL benennt somit ausdrücklich die Datenpreisgabe als entgeltliche Gegenleistung für das Bereitstellen digitaler Inhalte.

Dabei ist jedoch Art. 3 Abs. 4 DIRL als Bereichsausnahme zu berücksichtigen. Demnach gilt die Richtlinie nicht für Verträge über digitale Inhalte, die gegen eine andere Leistung als Geld bereitgestellt werden, soweit der Anbieter vom Verbraucher personenbezogene Daten verlangt, „*deren Verarbeitung für die* ***Erfüllung des Vertrags oder die Erfüllung rechtlicher Anforderungen unbedingt erforderlich ist, und er diese Daten nicht in einer mit diesem Zweck nicht zu vereinbarenden Weise weiterverarbeitet****. Sie gilt gleichfalls nicht für alle anderen Daten, die der Anbieter vom Verbraucher verlangt, um sicherzustellen, dass die digitalen Inhalte vertragsgemäß sind oder den rechtlichen Anforderungen entsprechen; diese Daten dürfen vom Anbieter nicht für kommerzielle Zwecke verwendet werden.*“

Dieser Ausschluss des Anwendungsbereichs wird der notwendigen Differenzierung gerecht, dass Datenverarbeitungen, die gesetzlich erlaubt und notwendig sind, etwa zur vertraglichen Abwicklung, nicht als schuldrechtliche Gegenleistungen angesehen werden können. Daten sind demnach nur dann als wirtschaftliche Gegenleistung einzuordnen, wenn sie auch als solche genutzt werden bzw. wenn sie über das unbedingt Erforderliche hinausgehen. In der Praxis müsste hier genau zu prüfen sein, ob dieser Ausschlusstatbestand missbräuchlich angewendet wird.

Die DIRL versucht also, auch die Verbraucher, die keine Gegenleistung in Geld erbringen, in eine mit dem zahlenden Kunden vergleichbare Position zu bringen.[7] Festgehalten werden kann, dass durch Art. 3 DIRL bestimmte Daten als Gegenleistung für das Bereitstellen digitaler Inhalte normiert werden, damit aber weitgehend Neuland betreten wird, da es keine nationalen gesetzlichen Vorbilder für diese Regelung gibt. Positiv zu beurteilen ist, dass sich nun alle Rechtsordnungen der Mitgliedstaaten hierzu positionieren müssen.[8]

b. Nationale Regelungen

Die Verbraucherschutzvorschriften der §§ 310 ff. BGB beruhen zwar auf der Verbraucherrechterichtlinie, deren Ziel die Vollharmonisierung ist. Dennoch verbietet es die Verbraucherrechterichtlinie nicht, weitere Vertragstypen in die Vorschriften über Verbraucherverträge aufzunehmen.[9]

Fraglich ist daher, ob Daten als entgeltliche Gegenleistung bereits jetzt vom Anwendungsbereich deutscher Vorschriften erfasst sind. Denn durch die Anwendung der Vorschriften über die Verbraucherverträge könnten Unternehmer, die eine Leistung gegen „Datenzahlung“ anbieten, dazu verpflichtet werden, verbraucherschützende Vorschriften einzuhalten. Sie müssten demnach Informationspflichten erfüllen oder gar im Rahmen der Buttonlösung auf die Zahlung mit Daten hinweisen. Dafür müssten diese Verträge allerdings den Verbrauchervertragsvorschriften unterstehen. Alternativ wäre zu überlegen, die Datenhingabe als weiteren Vertragstyp in die Vorschriften über die Verbraucherverträge aufzunehmen.[10]

- **Datenhingabe im Anwendungsbereich der §§ 312 Abs. 1, 310 Abs. 3 BGB**

§ 312 Abs. 1 BGB lautet: „*Die Vorschriften der Kapitel 1 und 2 dieses Untertitels sind nur auf Verbraucherverträge im Sinne des § 310 Abs. 3 anzuwenden,* ***die eine entgeltliche Leistung*** *des Unternehmers zum Gegenstand haben.*“ Dies entspricht auch der oben erläuterten Auslegung der VRRL durch den deutschen Gesetzgeber. Dem Wortlaut nach sind die Regelungen der §§ 310 ff. BGB also nur anzuwenden, wenn Gegenstand des Vertrages eine entgeltliche Leistung ist.

Unter „Entgelt“ versteht man zwar üblicherweise den Preis, Lohn, Honorar, Vergütung und Gebühr.[11] Daten als Gegenstand von Verträgen sind dem Wortlaut nach zunächst nicht erfasst. Jedoch ist der Begriff des Entgelts weit auszulegen.[12] Es genügt jede Leistung des Verbrauchers[13], weshalb teilweise vertreten wird, dass auch die Hingabe von Daten ein Entgelt darstellt.[14] Dies entspricht auch dem gesetzgeberischen Willen. Zwar lehnte der Gesetzgeber die Erstreckung der Vorschriften auf unentgeltliche Verträge – wie bereits dargestellt – ausdrücklich ab.[15] Gleichwohl bestätigt er ebenso, dass der Begriff des „Entgelts“ weit auszulegen sei. So ist der Gesetzesbegründung zu entnehmen:

Schließlich schränkt das Merkmal „entgeltliche Leistung“ den Anwen-

dungsbereich der Vorschriften auch nicht zu weitgehend ein. Insbesondere erfordert es nicht, dass das Entgelt in der Zahlung eines Geldbetrags liegt. Vielmehr ist das Merkmal „Entgelt“ weit auszulegen. (…) Es muss sich also um einen gegenseitigen bzw. einen Austauschvertrag handeln. Auf die Gleichwertigkeit von Leistung und Entgelt kommt es nicht an. Daher können Verträge, bei denen der Verbraucher für die Erbringung einer Dienstleistung (...) im Gegenzug personenbezogene Daten mitteilt und in deren Speicherung, Nutzung oder Weitergabe einwilligt, erfasst sein. Lediglich Verträge, bei denen überhaupt keine Gegenleistung geschuldet wird, sind demnach vom Anwendungsbereich ausgenommen.[16]

3. Lösungsansätze

Werden personenbezogene Daten bislang gegen Geld oder geldwerte Vorteile ausgetauscht, dann geschieht dies auf vertraglicher Grundlage, wie etwa die Kundenbindungssysteme[17], Nutzung sozialer Netzwerke oder Apps. Der Nutzer stellt hierfür seine Daten zur Verfügung, teilweise, weil sie für die Erfüllung des Vertrages oder die Nutzung der Dienstleistung erforderlich sind, teilweise aber auch darüber hinausgehend. Somit handelt es sich bei der kommerziellen Verwertung von Daten, die als Gegenleistung im Rahmen eines Vertrages eingesetzt werden, um eine dem Schuldrecht typische Austauschbeziehung.

Zwangsläufig sind aber auch datenschutzrechtliche Belange zu beachten, da das informelle Selbstbestimmungsrecht des Nutzers hinsichtlich der Nutzung seiner Daten betroffen ist. Grundsätzlich lässt sich festhalten, dass das Datenschutzrecht dem Persönlichkeitsschutz dient. So kommt man zu dem Ergebnis, dass bei der Ausgestaltung eines Datenschuldrechtes das Datenschutzrecht zwingend Berücksichtigung finden muss.

- **Nur bestimmte Daten als Gegenleistung**

Die kommerzielle Verwertung personenbezogener Daten ist grundsätzlich mangels gesetzlichen Erlaubnistatbestandes nur mit Einwilligung des Betroffenen möglich. Dies ergibt sich auch aus Art. 6 der Datenschutzgrundverordnung (DSGVO). Danach besteht ein generelles Verbot der Verarbeitung personenbezogener Daten mit Erlaubnisvorbehalt. Erlaubt ist die Verarbeitung personenbezogener Daten, wenn sie aufgrund Einwilligung des Betroffenen gemäß Art. 7 DSGVO erfolgt, oder aber das Gesetz die Datenverarbeitung gemäß Art. 6 Abs. 1 lit. b bis f DSGVO oder gemäß Art. 6 und 9 der RL 2002/58/EG erlaubt.[18]

Daher sollte die Hingabe von Daten zur kommerziellen Verwertung, welche aufgrund einer Einwilligung des Betroffenen stattfindet, als vertragliche Gegenleistung im Sinne der §§ 310 ff. BGB angesehen werden. Auf das Erfordernis einer aktiven Übermittlung oder Verschaffung von Daten sollte verzichtet werden. Dieses ist für die Einräumung der Nutzungsbefugnis durch die Einwilligung gerade nicht erforderlich.[19]

- **Widerruf und Rückabwicklung**

Bei der Ausgestaltung eines Datenschuldrechts darf nicht unberücksichtigt bleiben, dass dem Verbraucher gemäß Art. 7 Abs. 3 DSGVO jederzeit der Widerruf der Einwilligung möglich ist, mit der Folge, dass ihm ein Löschungsanspruch im Hinblick auf seine personenbezogenen Daten zusteht, Art. 17 Abs. 1 DSGVO. Hier ist zu überlegen, wie sich ein Widerruf der datenschutzrechtlichen Einwilligung auf das Vertragsverhältnis der Parteien auswirkt.[20] Sinnvoll erscheint eine gesetzliche Regelung, die den Anbieter im Falle eines Widerrufs oder der sonstigen Vertragsbeendigung dazu verpflichtet, digitale Inhalte zurück zu gewähren und Daten bei Vertragsende oder im Falle einer Rückabwicklung zu löschen.[21] Auch eine Klarstellung dahingehend, dass ein Widerrufsverzicht nicht möglich ist, erscheint sinnvoll.[22] Zu überlegen wird ebenfalls sein, ob und in welcher Form der Anbieter im Falle eines Widerrufs der datenschutzrechtlichen Einwilligung die Möglichkeit erhält, sich von dem schuldrechtlichen Vertrag zu lösen.

Daten als Entgelt: Anwendung der verbraucherschützender Vorschriften

Es erscheint folgerichtig, zunächst eine Klarstellung in § 312 BGB vorzunehmen und Daten im oben genannten Sinn unter Einwilligungsvorbehalt ausdrücklich als Entgelt im Rahmen des Verbrauchervertrages anzuerkennen. Daneben könnten datenschuldrechtliche Spezialvorschriften geschaffen werden, auf welche dann verwiesen werden kann. Die Notwendigkeit der Schaffung eines neuen Vertragstypen wäre vorläufig nicht gegeben.

Dies hätte zur Folge, dass der Unternehmer nicht nur die vertraglichen essentialia negotii angeben müsste. Ihn würden auch die **Informationspflichten nach § 312 d BGB, Art. 246 a EBGBG, Art. 8, 6 Abs. 1 VRRL** treffen. Demnach ist neben den „wesentlichen Eigenschaften der Dienstleistung“ etwa auch über den „Gesamtpreis“ sowie die „Art der Preisberechnung“ und die „Leistungsbedingungen“ zu informieren, § 312 d BGB i.V.m. Art. 246 a Abs. 1 Nr. 1, Nr. 4, Nr. 7 EGBGB. Dies könnte zur Folge haben, dass sowohl der kommerzielle Zweck für den die erhobenen Daten verwendet werden sollen, angegeben werden muss, als auch die Art und Unterart der hiervon betroffenen Daten (Bestandsdaten, wie etwa Name, Anschrift, E-Mailadresse, Nickname oder etwa auch Verkehrsdaten, wie die IP-Adresse). Die datenschutzrechtliche Einwilligungserklärung wäre in dem Vertragsverhältnis demnach nicht mehr ausreichend.

Zudem ist vorstellbar, dass die Hingabe von Daten als Entgelt für die kommerzielle Nutzung des Unternehmers auch eine Abbildung in der Buttonlösung **§ 312 j BGB, Art. 8 VRRL** erfährt.

Die diesbezüglichen Formulierungen beziehen sich aktuell ausschließlich auf Verträge, bei denen der Verbraucher als Gegenleistung „Zahlung“ erbringt. Daher lauten die zulässigen „Buttonformulierungen“ auf Grundlage des Art. 8 Abs. 2 VRRL aktuell gemäß § 312 j Abs. 3 S. 1 BGB insbesondere „zahlungspflichtig bestellen“ und „kostenpflichtig bestellen“.

Es ist angezeigt, hier im Falle eines Datenschuldvertrages eine Klarstellung in § 312 j Abs. 3 BGB aufzunehmen. Die zugrundeliegende VRRL lautet in Art. 8 Abs. 2 wie folgt:

Der Unternehmer sorgt dafür, dass der Verbraucher bei der Bestellung

ausdrücklich bestätigt, dass die Bestellung mit einer Zahlung verbunden ist.

Nach der hier vertretenen Ansicht, stellt die Gegenleistung mit Daten eine „Zahlung“ dar. Gibt der Verbraucher als Gegenleistungen also seine Einwilligung in die Verwendung seiner Daten für kommerzielle Zwecke, so sollte sich seine Vertragserklärung auch auf diesen Umstand beziehen. Als Buttonformulierung wäre daher durchaus denkbar: „*datenpflichtig bestellen*“.

Dies würde auch mit Blick auf den Sinn und Zweck der Preisangabenverordnung konsequent erscheinen. Danach wird das Ziel verfolgt, durch eine sachlich zutreffende und vollständige Verbraucherinformation Preiswahrheit und -klarheit zu gewährleisten, durch optimale Preisvergleichsmöglichkeiten die Stellung der Verbraucher gegenüber Handel und Gewerbe zu stärken und den Wettbewerb zu fördern.[23]

4. Konsequenzen eines Datenschuldrechts auf den Verbraucherschutz

Es lässt sich festhalten, dass die verbraucherschützenden Vorschriften des BGB entgeltliche Verträge erfassen und nach der wohl herrschenden Meinung unter „Entgelt“ auch die Hingabe von Daten zu verstehen ist. Jedoch scheint die ausdrückliche Aufnahme dieses Umstandes in den Wortlaut der Norm angebracht, da dies aus der Norm selbst nicht hervorgeht und hier Klarstellung geboten ist.[24] Insbesondere besteht das Erfordernis der Konkretisierung auch im Hinblick darauf, welche Daten als schuldrechtliche Gegenleistung anzusehen sind.

Dies hätte erhebliche positive Auswirkungen auf den Verbraucherschutz sowie letztlich auch auf den Datenschutz und würde zu einem transparenteren Wettbewerb führen. Würden Daten ausdrücklich als Währungstyp oder kaufähnliche Gegenleistung anerkannt, könnten Verbraucher hiervon in erheblichem Umfang profitieren.

Denn müssten alle Unternehmer, die ihre Dienstleistungen „geldfrei“ gegen „Datenzahlung“ anbieten, über den Preis und die wesentlichen Eigenschaften entsprechend der geltenden Vorschriften informieren, würde der Markt auf Dauer für den Verbraucher deutlich transparenter und die Diensteanbieter vergleichbarer werden.

Aufgrund der zur Verfügung gestellten Informationen könnten die Angebote und Preise der Diensteanbieter durch den Nutzer direkt verglichen werden. Dies hätte zur Folge, dass auf Unternehmerseite der Wettbewerb angeregt würde, datengünstige Angebote zu entwickeln, da der Verbraucher die verschiedenen Anbieter gerade mit Blick auf das Ausmaß der Datenerhebung und Verwendung auswählen könnte, gerade so, als würde hier der „Preis“ verglichen werden.

Letztendlich könnte der Verbraucher seinen Datenschutz aktiv selbst in die Hand nehmen, in dem er in die Lage versetzt wird, bei mehreren unterschiedlichen Angeboten dasjenige zu wählen, das den geringsten „Preis“ verlangt, also die wenigsten Daten nutzt. Und schließlich würde es der Ausgangsaussage gerecht werden, indem der „Zahlung mit seinen Daten“ eine rechtliche Entsprechung vorläge.

1 Müller/Rosenbach/Schulz, Die gesteuerte Zukunft, DER SPIEGEL 20/2013, S. 65 (67, 74).

2 Vgl. etwa die Plattform http://handshake.uk.com/hs/index.html, auf der Nutzer mit ihren Daten Geld machen können (abgerufen am 16.12.2016).

3 Loos/Helberger/Guibault/Mak, ERPL 2011, S. 729 (750).

4 Bt.-Drs. 17/13951, S. 72.

5 Bt.-Drs. 17/13951, S. 72.

6 KOM 2015 (643).

7 Die Richtlinienvorschläge der Kommission zu Verträgen über digitalen Inhalt und Online-Warenhandel, S. 1, abrufbar unter: https://www.bundestag.de/blob/422554/6f0bd347b413226ad2ffe992dc5cfa9f/bokor-data.pdf.

8 So Schmidt-Kessel, F. 16, https://www.bmjv.de/SharedDocs/Downloads/DE/Praesentationen/05032016_digitalesVertragsrecht_Schmidt_Kessler.pdf?__blob=publicationFile&v=1 (abgerufen am 22.12.16).

9 Grüneberg, in: Palandt, § 312, Rn. 1.

10 Grüneberg, in: Palandt, § 312, Rn. 1.

11 Grüneberg, in: Palandt, § 312, Rn. 3

12 Wendehorst, NJW 2014, S. 577 (580).

13 Grüneberg, in: Palandt, § 312, Rn. 3; Schirmbacher, in: Spindler/Schuster, § 312, Rn. 27; BGH, NJW 2003, S. 1190 (1191).

14 Brönneke/Schmidt, VuR 2014, S. 3 (3); a.A. Schirmbacher, in: Spindler/Schuster, § 312, Rn. 30.

15 Bt.-Drs. 17/13951, S. 71.

16 Bt.-Drs. 17/13951, S. 72.

17 Köhler, in: Bornkamm/Köhler, § 3, Rn. 8.51-8.52.

18 Insbesondere findet Art. 6 Abs. 1 lit. b DSGVO, der die Datenverarbeitung zur Erfüllung eines Vertrages erlaubt, keine Anwendung, wenn allein die kommerzielle Datennutzung Zweck des Vertrages ist, hierzu Art. 7 Abs. IV DSGVO, sowie Schmidt-Kessel, F. 5, https://www.bmjv.de/SharedDocs/Downloads/DE/Praesentationen/05032016_digitalesVertragsrecht_Schmidt_Kessler.pdf?__blob=publicationFile&v=1 (abgerufen am 22.12.16).

19 Schmidt-Kessel, a.a.O., F. 11.

20 Zu den ofenen Sachfragen überblickhalber kurz auch Schmidt-Kessel, a.a.O., F. 15.

21 71. DJT, Beschluss A.I.6.

22 Weitere Ausführungen hierzu Schmidt-Kessel, a.a.O., F. 12.

23 BGH, Urteil vom 31. Oktober 2013 -I ZR 139/12 -2 Flaschen GRATIS; m.V.a. BGH, Urteil vom 4. Oktober 2007 I ZR 143/04, GRUR 2008, 84 Rn. 25 = WRP 2008, 98 Versandkosten; Urteil vom 7. März 2013 I ZR 30/12, GRUR 2013, 850 Rn. 13 = WRP 2013, 1022 Grundpreisangabe im Supermarkt.

24 Vgl. nur den Antrag der Grünen im Rahmen des Gesetzgebungsprozesses Bt.-Drs. 17/13951, S. 59 aus dem ersichtlich davon ausgegangen wurde, dass „entgeltliche“ Verträge nicht solche mit Daten als Gegenleistung sind und daher ein Verstoß gegen die VRRL vorliege.

Tatjana Halm ist Referatsleitern des Bereichs Markt und Recht in der Verbraucherzentrale Bayern:

Ich danke an dieser Stelle Frau Julia Berger, Rechtsanwältin und Juristin in der Verbraucherzentrale Bayern für die Unterstützung bei der Recherche zu diesem Thema.

Stefan Ernst

Die Einwilligung des Minderjährigen in der DS-GVO

Minderjährige genießen in diversen Rechtsgebieten zu Recht besonderen Schutz. Dazu gehören das allgemeine Vertragsrecht des Bürgerlichen Gesetzbuchs (BGB), das Lauterkeitsrecht des UWG[1] und auch das Datenschutzrecht, wo dies in der Datenschutz-Grundverordnung (DS-GVO) ausdrücklich festgeschrieben wird. Der Beitrag diskutiert einige der relevanten Fragen.

I. Die Definition des Minderjährigen im Datenschutzrecht

Obwohl Kinder in Bezug auf ihre personenbezogenen Daten besonderen Schutz verdienen, weil sie sich der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten in der Regel (noch) weniger bewusst sind als Erwachsene[2], wird dieser Begriff in der DS-GVO zwar mehrfach verwendet[3], nicht aber definiert. Die DS-GVO geht ersichtlich davon aus, dass eine Einwilligung „im Kindesalter gegeben" werden kann.[4] Es kommt bei Minderjährigen daher sowohl eine durch einen Erziehungsberechtigten erteilte Erklärung in Betracht – hier wird das Prinzip der Höchstpersönlichkeit einer Einwilligung durchbrochen – als auch unter bestimmten Voraussetzungen eine Gestattung durch den Minderjährigen selbst.

Die im deutschen Recht zuweilen vorgenommene Unterscheidung zwischen Kindern und Jugendlichen findet sich in der DS-GVO nicht. Vielmehr wird hier letztlich allein von „Kindern" gesprochen. Art. 8 Abs. 1 DS-GVO gibt jedoch eindeutige Anhaltspunkte darauf, dass mit „Kindern" alle Personen unter 18 Jahren gemeint sind.

Art. 8 Abs. 1 DS-GVO sieht bei der Einwilligungsfähigkeit in Bezug auf Dienste der Informationsgesellschaft eine Regelgrenze von 16 Jahren vor. Aber auch bei Präventions- oder Beratungsdiensten, die unmittelbar einem Kind angeboten werden, geht Erwägungsgrund (EG) 38 davon aus, dass eine Einwilligung des Trägers der elterlichen Verantwortung nicht erforderlich sei. Dies bezieht sich kaum auf Dienste der Informationsgesellschaft[5] (in Art. 8 DS-GVO findet sich auch kein Hinweis hierzu), gründet aber wohl in der Annahme, dass solche Dienste nicht selten aufgrund von Problemen mit den Eltern in Anspruch genommen werden. Gleichzeitig setzt Art. 8 Abs. 2 DS-GVO eine absolute Untergrenze von 13 Jahren. Ein Kind, das noch keine 13 Jahre alt ist, kann also selbst keinerlei datenschutzrechtliche Einwilligung geben.

Im deutschen Recht wurde bislang in erster Linie auf die Einsichtsfähigkeit abgestellt[6], was durchaus sachgerecht ist und bei Jugendlichen unter 16 Jahren im Wesentlichen zu gleichen Ergebnissen führen wird. Auch die DS-GVO geht im Grundsatz davon aus, wenn sie zu einer wirksamen Einwilligung das Verständnis der erforderlichen Erklärungen voraussetzt. Die Tatsache, dass bei Diensten der Informationsgesellschaft eine Grenze von 16 Jahren angesetzt wird, bei denen die Jugendlichen eine Einwilligung ohne Einfluss der Eltern abgeben können sollen, bedeutet nicht, dass dies bei anderen Angeboten nicht möglich ist. Es ist aber in strengem Maße darauf zu achten, dass sowohl eine Einwilligungsfähigkeit im Allgemeinen als auch ein Verständnis für die Implikationen des konkreten Falles vorhanden sind. Beruft sich der Verarbeiter auf das Vorhandensein von Einwilligungen 16-Jähriger, ist das Transparenzerfordernis (dazu s. u. IV.) bezogen auf diese Altersklasse zu prüfen. Die Verständlichkeit der Formulierung muss also höher sein als bei Erwachsenen als Zielgruppe. Davon kann bei der überwiegenden Zahl von „Datenschutzerklärungen" in der Praxis leider nicht die Rede sein. Ob Jugendliche im Einzelfall von ihrer Reife her einwilligungsfähig sein können – im Rahmen von Art. 8 DS-GVO mit 16 Jahren generell definiert – schließt höhere Anforderungen bei der Transparenz nicht aus. Letztlich wird diese nicht nur von der Einsichtsfähigkeit der Altersklasse allein abhängen. Sie ist bezogen auf den konkreten Fall und damit in Bezug auf Inhalt und Reichweite der Einwilligung festzustellen.

Auf die genaue Rechtsnatur der Einwilligung (rechtsgeschäftliche Erklärung oder Realakt) kommt es angesichts der eindeutigen Regelungen nicht an, da die Geschäftsfähigkeit des Betroffenen insoweit keine Rolle spielt. Der Bundesgerichtshof (BGH) sieht sie im Rahmen des Bildnisrechts als bloßen Realakt an.[7] Letzteres ist aus praktischen Gesichtspunkten fast zwingend, da sonst jedes online gestellte Foto vom Kindergeburtstag bis zur Party unter 17-Jährigen von den Eltern genehmigt werden müsste. Bei der Annahme der Einwilligung eines Minderjährigen ist in diesem Zusammenhang aber in jedem Einzelfall genau festzustellen, ob dieser über die erforderliche Einsichtsfähigkeit hinsichtlich der tatsächlich möglichen Reichweite seiner Zustimmung verfügt.[8] Bei Kindern unter 14 Jahren würde diese allerdings ohnehin wohl generell fehlen.

II. Besondere Regelung der DS-GVO in Bezug auf TK- und Online-Dienste

Art. 8 der DS-GVO stellt besondere Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft (information society service) auf. Was diese sind, wird in Art. 4 Nr. 25 DS-GVO mit einer Bezugnahme auf eine andere EU-Richtlinie definiert.[9] Diese Definition umfasst jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung.[10] Letztlich umfasst dies alle in Bezug auf Datenerhebungen interessanten Telekommunikations- und Online-

dienste (inkl. der besonders erhebungsfreudigen sozialen Netzwerke, Messenger-Dienste und Suchmaschinen). Dabei ist es unerheblich, ob diese im konkreten Fall gegen Entgelt erbracht werden, denn derartige Dienste werden grundsätzlich nicht kostenfrei betrieben. Auch die in den jeweiligen Allgemeinen Geschäftsbedingungen (AGB) verlangte Gegenleistung der Preisgabe personenbezogener Daten ist im Übrigen bereits als Entgelt zu werten.

Art. 8 Abs. 1 DS-GVO statuiert zunächst, dass eine Einwilligung nach Art. 6 Abs. 1 lit. a DS-GVO nur ab dem 16. Lebensjahr erklärt werden kann.[11] Davor ist die Verarbeitung nur rechtmäßig, sofern und soweit diese Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wird.

Art. 8 Abs. 2 DS-GVO bestimmt ferner, dass der Verantwortliche unter Berücksichtigung der verfügbaren Technik angemessene Anstrengungen unternehmen muss, um sich in solchen Fällen zu vergewissern, dass die Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wurde. Hierfür wird das bloße Ankreuzen eines Feldes „Ich bin über 16" ebenso wenig ausreichen wie ein Kreuzchen bei einem Feld „Meine Eltern haben zugestimmt".[12] Vielmehr wird eine Art Double-Opt-In-Verfahren durch eine Rückfrage bei den Eltern zumutbar und nötig sein.[13] Hier steht allerdings das Problem im Raum, dass eine vom Jugendlichen angegebene E-Mail-Adresse kaum verlässlich dem Erziehungsberechtigten zuzuordnen wäre.[14] Weitere Angaben werden daher zur Verifizierung erforderlich werden. Das Risiko des Fehlens einer wirksamen Einwilligung liegt ohnehin beim Verantwortlichen (Art. 7 Abs. 1 DS-GVO).[15]

III. Der Referentenentwurf zum Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (DSAnpUG-E)

Kinder finden ferner Erwähnung im Entwurf zu § 14 Abs. 1 Nr. 2 DSAnpUG-EU, nach dem der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit u. a. die Aufgabe besitzt, die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung zu sensibilisieren und sie darüber aufzuklären. Im zweiten Satz heißt es dann ausdrücklich: „Besondere Beachtung finden dabei spezifische Maßnahmen für Kinder". Weitere Äußerungen oder Regelungen zum Thema Minderjährige finden sich im Referentenentwurf nicht. Der Schutz der unter 18-Jährigen richtet sich also allein nach der DS-GVO. Zu den Aufgaben des Bundesdatenschutzbeauftragten gehört demnach das Erstellen von Broschüren, mit denen Jugendliche über die Risiken der Preisgabe von personenbezogenen Daten besonders aufgeklärt werden.

IV. Die Einwilligung des Minderjährigen in AGB

Auch und gerade im Bereich Minderjährige wird eine Einwilligungserklärung in der Regel klauselmäßig vorformuliert sein. Dies ist vom Grundsatz her unbedenklich, in der Praxis aber in vielen Fällen nicht nur äußerst problematisch, sondern geschieht viel zu häufig schlicht nicht gesetzeskonform. Die für alle Betroffenen gleichermaßen geltenden Fragen zur Einwilligung (z. B. die Koppelung der Einwilligung oder eine kartellähnliche Angebotslage und ihre Widerruflichkeit) sollen hier nicht diskutiert werden.[16]

1. Grundsätzliches

Grundsätzlich ist die Verwendung von vorformulierten Einwilligungserklärungen selbst dann möglich, wenn sich diese zusammen mit anderen Aspekten in AGB finden. Hierfür gilt zunächst Art. 7 Abs. 2 DS-GVO, wonach die datenschutzrechtliche Einwilligung zum einen in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache und zum zweiten so zu erfolgen hat, dass sie von den anderen Sachverhalten klar zu unterscheiden ist. Die Datenschutzklausel in den AGB muss demnach besonders hervorgehoben werden. Es bedeutet gleichzeitig, dass der Nutzer zumindest den Hinweis erhalten muss, dass sich innerhalb der AGB auch eine datenschutzrechtliche Einwilligung verbirgt. Fehlt es daran, liegt keine Einwilligung vor.[17] Das schlichte „Ich stimme den AGB zu", das im allgemeinen Vertragsrecht ansonsten ausreichend ist, genügt daher nicht.

2. Möglichkeit zur Kenntnisnahme

Die Abgabe der von Art. 4 Nr. 11 DS-GVO für eine wirksame Einwilligung verlangten informierten Erklärung (die Entwurfsversion sprach von einer „Erklärung in Kenntnis der Sachlage") setzt voraus, dass der Betroffene die Möglichkeit hat, den Inhalt der von ihm erwarteten Erklärung in zumutbarer Weise zur Kenntnis zu nehmen. Dies hat besondere Bedeutung bei vorformulierten Einwilligungen im Rahmen von AGB und „Datenschutzerklärungen", die ebenfalls als AGB zu werten sind.

Versteckte Hinweise, technische Textformate, die nicht jedem Nutzer zugänglich sind oder undeutliche Schriftarten können diese Zumutbarkeit ebenso hindern wie überlange Texte. Erklärungen über mehrere Seiten sind nur dann zumutbar, wenn dieser Umfang tatsächlich erforderlich ist, um den Sachverhalt zu erläutern. Die Lektüre von AGB mit mehreren DIN-A4-Seiten Inhalt ist schlicht unzumutbar[18], wobei es dann auch keine Rolle spielt, wenn die darin enthaltene und hinreichend hervorgehobene (Art. 7 Abs. 2 DS-GVO) datenschutzrechtliche Einwilligung kurz ist. Anderenfalls besteht nicht nur der Verdacht, dass der Verwender von der Lektüre abschrecken möchte, sondern es fehlt letztlich schlicht an der Zumutbarkeit der Kenntnisnahme.

An einer Zumutbarkeit fehlt es auch, wenn der Betroffene die Erklärungen an mehreren unterschiedlichen Stellen oder nur anhand von mehrstufigen Verweisen findet. Die Verwendung mehrerer Klauselwerke, gleich ob nebeneinander oder kaskadenartig, ist geeignet, die Einbeziehung der gesamten Regelungen mangels Zumutbarkeit der Lektüre und mangels Transparenz zu verhindern. In solchen Fällen spielt es auch keine Rolle, ob der Nutzer ein Kästchen „Ich bin mit den AGB einverstanden" oder womöglich noch mit dem unsinnigen Zusatz „Ich habe die AGB verstanden" angekreuzt hat.

3. Transparenzgebot

Kenntnis der Sachlage verlangt zugleich, dass die entsprechende Erklärung verständlich ist, da sonst von einer informierten Einwilligung nicht die Rede sein kann (siehe auch Art. 5 Abs. 1 lit. a[19] und Art. 12 DS-GVO). Hiermit ist nicht nur eine verständliche Sprache gemeint, sondern auch die Abwesenheit unnötigen technischen oder fremdsprachigen Fachvokabulars, dessen Bedeutung nicht allen potentiellen Adressaten ohne Weiteres bekannt ist.

Dies ist bei Minderjährigen nicht unproblematisch, wobei unerheblich ist, ob diese „in der Regel von Technik mehr verstehen als Erwachsene“. Es geht nicht um das Verständnis der Technik, sondern um die Bedeutung der Einwilligungserklärung und ihrer Folgen. Wenn der Betroffene zu verstehen geben soll, dass er mit der Verarbeitung der ihn betreffenden personenbezogenen Daten einverstanden ist, muss er beim Lesen des Datenschutzhinweises in der Lage sein, diesen inhaltlich vollumfänglich zu erfassen. Möchte der Verarbeiter die Einwilligung eines 16-Jährigen einholen, muss er seine deren Reichweite erklärenden Hinweise entsprechend verständlich fassen. Für eine auf einen Minderjährigen zugeschnittene Einwilligungserklärung genügt es hier nicht, unpersönliche Formulierungen lediglich durch ein penetrantes „Du“ zu ersetzen („Mit der Teilnahme am sozialen Netzwerk stimmst du der Verwendung deiner Daten zu“ o. Ä.). Der betroffene Minderjährige muss vielmehr nach der Lektüre der Einwilligungserklärung klar wissen (können), wer nach der von ihm zu gebenden Einwilligung welche seiner Daten zu welchem Zweck und über welchen Zeitraum hinweg nutzen möchte.

4. Sprachproblem

An einer informierten Einwilligung fehlt es ferner, wenn diese nicht in einer für den Betroffenen verständlichen Sprache verfasst ist (vgl. Art. 7 Abs. 2 DS-GVO).[20] Damit ist vor allem die Verwendung von deutscher Sprache für deutsche Nutzer gemeint. Auch wenn die Kenntnis der englischen Sprache weit verbreitet ist, wäre das Erfordernis, die englische Rechtssprache zu begreifen, ein Kriterium, das die Transparenz hindert. Selbst deutsche Juristen, die des Englischen mächtig sind, verstehen nicht zwingend die Feinheiten der fremden Rechtssprache. Erwartet ein internationaler Anbieter von deutschen Nutzern eine datenschutzrechtliche Einwilligung, muss diese in deutscher Sprache gefasst sein.[21]

V. Fazit

Nicht zu Unrecht wird beklagt, dass die meisten Nutzer von Online-Diensten keine Ahnung haben, was mit ihren Daten wirklich geschieht. „Es beginnt immer mit dieser kleinen Lüge: Ich habe die Datenschutzbestimmungen gelesen und erkläre mich mit ihnen einverstanden“.[22] Und dies gilt umso mehr bei Jugendlichen. Wie wenig Verständnis schon für die Reichweite der offenen Datenverwendung bei Foto- und Videoportalen besteht, zeigt sich in den Peinlichkeiten, die dort publiziert werden.[23] Woher soll dann das Verständnis für die Bedeutung der sonstigen Verwendung dieser Inhalte durch den Portalbetreiber kommen, mit denen die Jugendlichen dann im schlimmsten Fall womöglich noch ein ganzes Leben lang umgehen müssen?

1 Gesetz gegen den unlauteren Wettbewerb; erwähnenswert ist in diesem Zusammenhang, dass der „Tausch“ von anderweitig kostenpflichtigen Leistungen gegen personenbezogene Daten seit der UWG-Reform als geschäftliche Entscheidung i. S. d. § 2 Abs. 1 Nr. 9 UWG einzuordnen ist (Köhler in Köhler/Bornkamm, UWG, 35. Aufl. 2017, § 2 Rn. 159; Ernst in jurisPK-UWG, 4. Aufl. 2016, § 2 Rn. 57; vgl. auch BGH GRUR 2014, 682 – Nordjob-Messe).

2 EG 38, 58, 65.

3 Art. 6, 8, 12, 40 und 57.

4 EG 65.

5 Frenzel in Paal/Pauly (Hg.), DS-GVO, 2016, Art. 8 Rn. 8.

6 S. etwa Däubler in DKWW, BDSG, 5. Aufl., § 4a Rn. 5 mwN.

7 BGH, NJW 1980, 1903, 1904; vgl. auch BGH CR 2010, 463 – Vorschaubilder I; CR 2012, 333 – Vorschaubilder II; zur Einordnung beim Bildnisrecht siehe etwa Dreier/Schulze § 22 KUG Rn. 16 ff.; Götting in Schricker/Loewenheim § 22 KUG Rn. 39 ff.; jeweils mwN.

8 Dazu Dreier/Schulze § 22 KUG Rn. 26; Götting in Schricker/Loewenheim § 22 KUG Rn. 42.

9 Im Sinne dieser Verordnung bezeichnet der Ausdruck „Dienst der Informationsgesellschaft“ eine Dienstleistung im Sinne des Artikels 1 Nummer 1 Buchstabe b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates.

10 Siehe dazu Ernst in Paal/Pauly (Hg.), DS-GVO, 2017, Art. 4 Rn. 142 ff.

11 Die Mitgliedstaaten können durch Rechtsvorschriften zu diesen Zwecken eine niedrigere Altersgrenze vorsehen, die jedoch nicht unter dem vollendeten dreizehnten Lebensjahr liegen darf (Öffnungsklausel des Art. 8 Abs. 1 Satz 3 DS-GVO). Im Referentenentwurf zum DSAnpUG-EU findet sich allerdings keine diesbezügliche Regelung. Kritisch zu dieser Öffnungsklausel Plath in Plath (Hg.), Art. 8 DS-GVO Rn. 9.

12 Frenzel in Paal/Pauly (Hg.), DS-GVO, Art. 8 Rn. 13; großzügiger Plath in Plath (Hg.), Art. 8 DS-GVO Rn. 12.

13 Frenzel in Paal/Pauly (Hg.), DS-GVO, Art. 8 Rn. 13.

14 Frenzel in Paal/Pauly (Hg.), DS-GVO, Art. 8 Rn. 13.

15 A. A. Plath in Plath (Hg.), Art. 8 DS-GVO Rn. 14.

16 Dazu siehe etwa Ernst in Paal/Pauly (Hg.), DS-GVO, Art. 4 Rn. 73 ff.

17 Ernst in Paal/Pauly (Hg.), DS-GVO, Art. 4 Rn. 8.

18 Vgl. auch Art. 5 Satz 1 RL 93/13 über missbräuchliche Klauseln in Verbraucherverträgen, umgesetzt in § 307 BGB.

19 „In einer für die betroffene Person nachvollziehbaren Weise ... Transparenz“; engl. Fassung: „in a transparent manner in relation to the data subject ... transparency“.

20 Siehe auch Art. 5 Satz 1 RL 93/13 über missbräuchliche Klauseln in Verbraucherverträgen, umgesetzt in § 307 BGB.

21 Vgl. LG Berlin CR 2014, 676 – WhatsApp, bestätigt durch KG v. 08.04.2016 – 5 U 156/14.

22 Salavati, SZ v. 08.08.2015.

23 Vgl. Ernst, NJW 2009, 1320, 1322.

Jacob Kornbeck[1]

Einwilligung oder gesetzliche Regelung?

Die Wahl der Rechtsgrundlage bei Datenübermittlungen der NADA Deutschland in Drittländer zu Anti-Doping-Zwecken gemäß EU-Datenschutz-Generalverordnung

"The legal status of data protection as a fundamental right is crucial to understanding the importance which Europeans give to it."[2]

1. Einleitung

1.1. Kontext und Fragestellung

Als in der EU tätige Nationale Anti-Doping-Organisation (NADO) muss auch die Stiftung Nationale Anti-Doping-Agentur (NADA) Deutschland Erwartungen der World Anti-Doping Agency (WADA) und ihrer *Stakeholder* – des IOC und sonstiger *Sport Governing Bodies* (SGBs) – im Hinblick auf Datenaustausch und Datenübermittlung entsprechen, ohne die in der EU geltenden datenschutzrechtlichen Vorgaben zu verletzen. Die Wahl der Rechtsgrundlage stellt dabei aufgrund des besonderen datenschutzrechtlichen Rechtmäßigkeitsvorbehalts nach Bundesdatenschutzgesetz (BDSG), EG-Datenschutz-Richtlinie 95/46/EG[3] (DS-RL) und (ab 2018) EU-Datenschutz-Grundverordnung (VO 2016/679)[4] (DSGVO) eine besondere Hürde dar. Während neben Einwilligung oder gesetzlicher Regelung auch noch durch einen individuellen Vertrag, Standardvertragsklauseln oder verbindliche konzerninterne Datenschutzvorschriften „geeignete Garantien“ geschaffen werden können, bezweckt die vorliegende Untersuchung eine vergleichende Analyse von Einwilligung und gesetzlicher Regelung nach den Vorgaben der DSGVO, da in Sport und Anti-Doping traditionell systematisch auf die Einwilligung rekurriert wird.[5] Dabei stellt in Deutschland seit dem 1.1.2016 für die NADA das Anti-Doping-Gesetz (AntiDopG)[6] eine gesetzliche Regelung besonderer Art dar, während die zunehmende Einbeziehung von Strafverfolgungsbehörden erlaubt, besonders für diesen Bereich geltende Rechtsgrundlagen in Anspruch zu nehmen.

Für die Arbeit der NADOs grundsätzlich (vorbehaltlich nationalen Rechts) maßgeblich sind der World Anti-Doping Code (WADC)[7], „kein förmliches Gesetz, sondern ein privatrechtlicher Leitcodex“[8], und die „International Standards“[9] (IS) der WADA, die auf eine weltweite Integration und Harmonisierung des Anti-Doping-Kampfes abzielen, selbst jedoch keine Rechtskraft besitzen. Denn die von sämtlichen EU-Mitgliedstaten ratifizierten Anti-Doping-Übereinkommen („Konventionen“) von Europarat[10] und UNESCO[11] überlassen den Vertragsstaaten die Wahl des Instruments zur Umsetzung ihrer völkerrechtlichen Verpflichtungen[12], und verpflichten lediglich zur „Einhaltung“ der „Regelungen des WADC“.[13] Auch das Unionsrecht (einschl. Art. 165 AEUV zum Sport) verpflichtet in keiner Weise zur Schaffung einer gesetzlichen Regelung. Einige Staaten haben die Bestimmungen des Codes per Gesetz oder Erlass ins nationale Recht integriert, jedoch ergibt sich EU-weit ein recht heterogenes Bild.[14] Das AntiDopG verweist *nicht* auf den WADC, sondern lediglich auf Anlage I zum UNESCO-Übereinkommen, die ausdrücklich keine völkerrechtliche Rechtskraft besitzt[15] und somit (anders als von der WADA vertreten[16]), selbst wenn national „übertragen“[17], nicht als Rechtsgrundlage der Datenverarbeitung dienen kann.

Vor diesem Hintergrund soll hier untersucht werden, wie sich die Frage „Einwilligung oder gesetzliche Regelung?“ nach den Vorgaben der DSGVO stellt. Bei der Würdigung der durch §§ 8-10 AntiDopG geschaffenen Möglichkeiten ist ferner auf Erwägungsgrund 112 (EG 112) DSGVO einzugehen, die ausdrücklich Genehmigungen für Datenübermittlungen zu Anti-Doping-Zwecken vorsieht, sowie auf die dabei vorzunehmende Rechtsgüterabwägung.

1.2 Forschungsstand

Erkannt wurde das Problempotential Anti-Doping/Datenschutz in politischen Kreisen ab 2008 im Zusammenhang mit der Verabschiedung des (2011 revidierten) WADA-Datenschutzstandards ISPPPI.[18] Als sich die Art.-29-Datenschutzgruppe (WP29) der nationalen Aufsichtsbehörden mit WADC- und ISPPPI-Normen befasste[19], folgten WADA/EU-Kommunikationsprobleme[20], doch bereits im Mai 2009 erkannte eine EU-weite Tagung mit WADA-Teilnahme die Probleme an[21]. Eine ähnliche EU-Tagung befasste sich im Juni 2016 (ebenfalls mit WADA-Teilnahme) mit den Implikationen der DSGVO.[22] Doch obwohl NADOs nicht erst 2009 begannen, Athletendaten zu verarbeiten, begann eine rechtswissenschaftliche Fachdiskussion relativ spät. Anfang der 2000er Jahre sollen in der Schweiz erstmals Datenverarbeitungsoperationen im Sport zum Gegenstand von Empfehlungen der kantonalen und eidgenössischen Aufsichtsbehörden geworden sein.[23] Der Autor einer Schweizer (arbeitsrechtlichen) Dissertation, *Flueckiger*[24], stellte schon vor 2009 gravierende Rechtsverletzungen durch SGBs und NADOs[25] sowie ein überraschend fehlendes Unrechtsbewusstsein hinsichtlich bestehender datenschutzrechtlicher Vorgaben[26] fest. Die Ursache dieser Problematik sah *Flueckiger* im bislang schwieri-

gen Zugang zu den Schweizer Gerichten und dem dadurch verursachten Eindruck der SGBs, nicht dem staatlichen Recht unterworfen zu sein.[27] *Flueckiger* erhoffte sich eine Bewusstseinsänderung der SGBs und einen künftig besseren Schutz der Athleten-Persönlichkeitsrechte[28] und widmete der Problematik der internationalen Datenübermittlung eine dreiseitige Darstellung aufgrund des Schweizer Datenschutzgesetzes sowie des Datenschutz-Übereinkommens des Europarats („Convention 108“).[29] Aus Deutschland sind zu unserem Thema bislang drei rechtswissenschaftliche Dissertationen bekannt. Trotz einiger Vorbehalte sahen *Niewalda*[30]und *Mortsiefer*[31], deren Werke von *Weichert*[32] stark kritisch bewertet wurden, das gegenseitige Verhältnis Anti-Doping-Reglements und Datenschutzrecht nicht als besonders problematisch an. Eine weniger vorteilhafte Einschätzung findet sich in der Dissertation der Ex-Handballspielerin *Neuendorf*[33], die auch persönliche Erfahrungen als ehemalige Spitzensportlerin mit einfließen ließ.[34] *Neuendorf* untersuchte die vor Inkrafttreten des AntiDopG in Deutschland geltende Regelung, als mangels gesetzlicher Regelung ausschließlich auf Athleteneinwilligungen zurückgegriffen wurde, die Verpflichtungen rein privatrechtlicher Natur waren und aufgrund dynamischer Verweisungen bestanden, welche „trotz ihrer Vorteile für das sportverbandliche System [...] einer gerichtlichen Kontrolle nicht standhalten würden“.[35] „Die umfängliche Verarbeitung [...] hochsensibler [insbes. medizinischer, J.K.] Daten lässt sich mit dem Interesse einer effektiven Dopingbekämpfung wohl kaum rechtfertigen“, so das Fazit der Dissertation, in der ein zukünftig besserer Schutz der informationellen Grundrechte der Athleten gefordert wird.[36]

Aus dem weiteren Schrifttum bekannt ist eine begrenzte Fachdiskussion insbesondere seit 2009[37], die teilweise mit der relativen Verbandsnähe der Autoren zusammenzuhängen scheint. So wunderte sich der Landesbeauftragte (LfD) für den Datenschutz des Landes Schleswig-Holstein (SH) *Weichert* (Mitherausgeber einer amtlichen Stellungnahme zur Problematik[38]) in einer Buchbesprechung[39] zur Dissertation von *Niewalda*[40] über dessen Rechtfertigung des Systems der Meldepflichten („Whereabouts“) und bezeichnete die ADAMS-Datenbank (Anti-Doping Administration and Management System) der WADA als „informationstechnisch großkalibriges, leider nicht besonders ausgeklügeltes Kontroll- und Überwachungssystem“, wohingegen er ein vom sportfernen Arbeitsrechtler *Wedde* (im Auftrag der Basketballspielergewerkschaft SPIN) erarbeitetes Rechtsgutachten[41] lobte. Die von internationalen Sportgewerkschaften veröffentlichten Forschungsberichte[42] und Stellungnahmen[43] schienen *Weichert* Recht zu geben. Vom Bundesdatenschutzbeauftragten a. D. *Schaar* liegt ebenfalls ein Manuskript vor.[44] Jüngst wurden in Deutschland die (nicht nur datenschutzrechtlich) bedenkliche Praxis zur Veröffentlichung von Anti-Doping-Test-Ergebnissen und -Sperren[45] sowie (vom Anti-Doping-Kampf losgelöst) die zunehmende Verwendung von „big data“ im Sport[46] diskutiert, während ein IT-Tool Namens *eves* kommentiert wurde.[47]

2. Einwilligung oder gesetzliche Regelung?

2.1. Datenschutzrechtliche Erfordernisse

Der Nachweis einer Rechtsgrundlage der Datenverarbeitung ergibt sich nach Art. 8 Abs. 2 EU-Grundrechtecharta[48], gestützt durch Art. 16 AEUV als zwingend erforderlich und ist im abgeleiteten Recht entsprechend normiert (Art. 7 DS-RL; Art. 6 Abs. 1 DSGVO; § 4 BDSG). Dieser „als erster erwähnte“ Grundsatz[49] entspricht einem seit dem 2. BDSG (1977) „vielfach“[50] beachteten „Verbot mit Erlaubnisvorbehalt“[51] der Erhebung, Verarbeitung und Nutzung personenbezogener Daten, „sofern nicht eine spezielle Erlaubnis durch Rechtsnorm bzw. durch den Betroffenen selbst erteilt ist“.[52] Fehlt eine gültige, über einfache Billigkeit (*fairness*) hinausgehende Rechtsgrundlage (*lawfulness*)[53] bleibt die Verarbeitung unzulässig[54], und die Zulässigkeit ist „in jedem Einzelfall sorgfältig und auf jede Phase der Erhebung, Verarbeitung bzw. Nutzung zu prüfen“.[55] Da in der EU das Recht auf Datenschutz Grundrechtstatus genießt und das Schutzniveau als eines der weltweit höchsten gilt[56] (und tendenziell Schule macht[57]), können Daten nur bedingt in so genannte Drittländer übermittelt werden, da dies sonst durch die weitere Verarbeitung zu Grundrechtsverletzungen durch unregulierte „data havens“[58] führen könnte.[59] Einzelne Bereiche können Ausnahmen nicht erwarten, selbst (oder gerade) wenn das Volumen ihrer Datenübermittlungen als umfassend gilt, wie dies bei den NADOs der Fall zu sein scheint.[60] Das Beispiel des EU-Freizügigkeitsrechts zeigt übrigens eindrucksvoll, dass es auf Dauer besser sein kann, sich proaktiv auf gesetzliche Vorgaben einzustellen: Die Fußballverbände wussten sehr wohl vor dem Bosman-Urteil des EuGH[61], dass die von ihnen vertretene Rechtsposition anfechtbar war, setzten aber lieber darauf, Bereichsausnahmen zu verlangen[62], was sie eine Niederlage vor Gericht kostete.

Nach Unionsrecht sowie nach deutschem Recht kann diesem Erfordernis durch gesetzliche Anordnung *oder* Einwilligung der betroffenen Person entsprochen werden. Diesem Raster folgen Art. 7 der DS-RL 95/46/EG sowie Art. 6 Abs. Abs. 1 DSGVO (beide: Rechtmäßigkeit der Verarbeitung), wobei im Unionsrecht neben der Einwilligung (Art. 6 Abs. 1 lit. a) die Fallgruppen gesetzlicher Anordnung enumerativ geregelt sind: b) Erfüllung eines Vertrags (lit. b); bzw. einer gesetzlichen Verpflichtung der verarbeitenden Stelle (lit. c); Schutz lebenswichtiger Interessen der betroffenen Person (lit. d); Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung hoheitlicher Gewalt (lit. e); Wahrung berechtigter Interessen der verarbeitenden Stelle, sofern dadurch keine Grundrechte der betroffenen Person verletzt werden (lit. f). Bei einer Verarbeitung zu Anti-Doping-Zwecken können wohl lediglich Einwilligung (lit. a) sowie ggf. öffentliches Interesse bzw. hoheitliche Gewalt (lit. e) bemüht werden. Bei lit. b) fällt auf, dass die WP29 bereits längst von einer wohlwollenden Auslegung im Arbeitsverhältnis Abstand nimmt (z. B. zentralisierte Personalverwaltung multinationaler Konzerne zur „Erfüllung“ des Arbeitsvertrags ihrer Mitarbeiter): „Schließlich besteht kein direkter und objektiver Zusammenhang zwischen

der Erfüllung eines Beschäftigungsvertrags und einer solchen Datenübermittlung".[63] Ein Ausnahmetatbestand liegt nur dann regelmäßig vor, wenn diese die betroffene Person begünstigt (z. B. Buchung von Hotel oder Mietwagen).[64] Auch bei Sportlern lässt sich diese Frage *mutatis mutandis* stellen. Bei (lit. a) (Einwilligung) freilich sind erhebliche datenschutzrechtliche Bedenken zu berücksichtigen, während bei (lit. e) vorerst eine entsprechende gesetzliche Regelung vorliegen muss.

Trotz einer expliziten Erwähnung in EG 112 DSGVO finden die üblichen Vorgaben und Beschränkungen Anwendung. Daten werden nicht einfach bereit gestellt (vgl. Lindquist[65]), sondern gesandt. Übermittlungen an einen WADA-Server in Kanada oder an sonstige Partnerorganisationen regeln Art. 44-50 (Kapitel V) DSGVO, während „für die etwaige Weiterübermittlung" in ein anderes Drittland oder an eine andere internationale Organisation das in der EU gewährte Schutzniveau nach EG 101[66] DSGVO „nicht untergraben werden" darf, weshalb nach Art. 44 die für die erste Übermittlung geltenden Erfordernisse (bei der die Daten erstmals die EU verlassen) weiterhin gelten. Die Bestimmungen der DSGVO gelten somit unbeschränkt.

Sofern die Europäische Kommission nach Anhörung der WP29 („Angemessenheitsbeschluss") festgestellt hat, dass ein Drittland, ein Gebiet oder eine internationale Organisation „ein angemessenes Schutzniveau" bietet, können Daten dorthin nach Art. 45 DSGVO ohne „besondere Genehmigung" transferiert werden. Solche Angemessenheitsbeschlüsse sind sehr selten[67] und können seit der Nichtigkeitsfeststellung[68] des EuGH zur Safe-Harbor-Regelung (einem EU-US-Rahmen zur Selbstzertifizierung aus dem Jahr 2000, an dem freilich schon viel früher Zweifel geäußert worden waren[69]) in der Rechtsprechung Schrems[70] nicht mehr als endgültig angesehen werden.[71] Auch der Angemessenheitsbeschluss[72] zum kanadischen Bundesgesetz PIPEDA (Personal Information Protection and Electronic Documents Act)[73], das jüngst ergänzt wurde, um explizit die WADA in dessen Anwendungsbereich aufzunehmen[74], kann nicht mehr als sicher angesehen werden, und die von der WP29 Ende 2015 angekündigte Option koordinierter Erzwingungsmaßnahmen („coordinated enforcement actions")[75] bleibt weiterhin relevant. Das am 29.02.2016 ausgehandelte EU-US-Abkommen „Privacy Shield"[76] bezweckt, dagegen Abhilfe zu verschaffen, führt auf US-Seite jedoch keine den in der EU geltenden vergleichbaren Rechtsbehelfe ein[77] und könnte möglicherweise mit Erfolg vor Gericht angefochten werden.[78] In der Tat wurde am 16.09.2016 von der NGO *Digital Rights Ireland* (die sich nach dem gleichnamigen Rechtsstreit[79] bereits großer Bekanntheit erfreut) eine entsprechende Nichtigkeitsklage eingereicht.[80] Gefordert wurde die Aufhebung der Kommissionsentscheidung (EU) Nr. 2016/1250 vom 12.07.2016 aufgrund eines vom Gericht festzustellenden erheblichen Ermessensfehlers („manifest error of assessment by the Commission insofar as it finds an adequate level of protection in the US, for personal data, concordant with Directive 95/46/EC"). Im *Schrems*-Urteil bestätigte der EuGH nicht nur das Recht, sondern auch die Pflicht der Aufsichtsbehörden, bei entsprechenden Klagen die Rechtmäßigkeit von Datenübermittlungen zu prüfen, *selbst wenn* ein Angemessenheitsbeschluss vorliegt.[81] Darüber hinaus herrschte bislang über Zuständigkeit und geltendes Recht (Kanada/Québec) Unklarheit, weshalb die WP29 das in der Provinz gewährte Schutzniveau untersuchte[82], jedoch ohne ein eindeutiges Votum abgeben zu können.

Sofern nicht gemäß Art. 45 DSGVO die Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses stattfinden kann, müssen „geeignete Garantien" nach Art. 46, „verbindliche interne Datenschutzvorschriften" (*binding corporate rules*) nach Art. 47 oder sonst „Standarddatenschutzklauseln" (*standard contractual clauses*) nach Art. 28 Absatz 2 und Art. 46 Absatz 2 lit. d) vorliegen. „Ausnahmen für bestimmte Fälle" sind in Art. 49 definiert, der weitgehend die in Art. 6 festgelegten Rechtmäßigkeitstatbestände wiederholt: Einwilligung der betroffenen Person (Art. 49 Abs. 1 lit. a), Erfüllung eines Vertrags (lit. b), Interesse der betroffenen Person (lit. c), wichtige Gründe des öffentlichen Interesses (lit. d), Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (lit. e), Schutz lebenswichtiger Interessen der betroffenen Person oder anderer Personen (lit. f), Übermittlung aus einem Register, das gemäß dem Recht der Union oder der Mitgliedstaaten zur Information der Öffentlichkeit bestimmt ist (lit. g). Aus dieser Auflistung kommen wohl nur die Einwilligung (lit. a) bzw. die Wahrnehmung eines öffentlichen Interesses[83] (lit. d) in Betracht. Auf die Einwilligung nach (lit. a) wird noch einzugehen sein (s. u.); dabei gelten besonders strenge Maßstäbe zur Sicherung der Ausübung der Rechte der betroffenen Person. Sofern keine der Vorschriften in Art. 45-46 DSGVO Anwendung finden und keine Ausnahmetatbestände beansprucht werden können, darf eine Übermittlung nur erfolgen, solange sie einmalig und der Personenkreis begrenzt ist; „für die zwingend berechtigten Interessen" der verarbeitenden Stelle als „erforderlich" gilt, ohne dabei die Interessen, Rechte und Freiheiten der betroffenen Person zu verletzten; und „angemessene Garantien" vorliegen. Die verarbeitende Stelle ist dann verpflichtet, die Aufsichtsbehörde sowie die betroffene Person zu unterrichten (Art. 49 Abs. 1 DSGVO).

2.2. Einwilligung als Rechtsgrundlage

Wie bereits erwähnt, findet sich unter den in Art. 49 Abs. 1 DSGVO genannten „Ausnahmen für bestimmte Fälle" die Einwilligung der betroffenen Person nach Art. 49 Abs. 1 lit. a). Die Erfüllung dieses besonderen Tatbestands setzt freilich voraus, dass „die betroffene Person [...] in die vorgeschlagene Datenübermittlung ausdrücklich eingewilligt [hat], nachdem sie über die für sie bestehenden möglichen Risiken derartiger Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien unterrichtet wurde" und unterliegt somit den geltenden Maßstäben der WP29 zur Einwilligung.

Die Rechtmäßigkeit der Übermittlung setzt schon die der Erhebungsphase voraus, wo bereits nach Art. 7 Abs. 1 DSGVO verschärfte Erfordernisse gelten. Der verarbeitenden Stelle obliegt der Nachweis, dass eindeutig festgelegte Zwecke verfolgt werden (lit. 1-3). Gerade in der heutigen Zeit erfolgt die Notwendigkeit einer „strengen Zweckbindung" aus der zunehmend „multi-

funktionalen Verwendung“ von Daten.[84] Die Einwilligung der betroffenen Person kommt dann nicht in Betracht, „wenn zwischen der Position der betroffenen Person“ und der verarbeitenden Stelle „ein erhebliches Ungleichgewicht besteht“ (EG 34)[85]. Dadurch hat der europäische Gesetzgeber einen über Jahrzehnte entstandenen Konsens kodifiziert, der auch durchgängig von der WP29 vertreten wurde und wird: „Die Richtlinie stellt die Einwilligung eindeutig als eine von mehreren Rechtsgrundlagen dar.“[86] Die in Deutschland gängige, als Verfassungsnorm geltende[87] Doktrin[88] der informationellen Selbstbestimmung scheint dem „erheblichen Ungleichgewicht“ vergleichbar, denn wie bei AGBs setzt Selbstbestimmung Durchsetzungsvermögen voraus.[89] Im Beschäftigungsverhältnis galt die Einwilligung gemäß der WP29 als ungültig, wenn sie „vom Beschäftigten erbeten und [...] die Nichteinwilligung mit tatsächlichen oder potenziellen Nachteilen für ihn verbunden“[90] wäre, was auch dem Tenor des deutschen Schrifttums entspricht.[91]

Entsprechend monierte die WP29 bereits 2008 anhand eines WADA-Entwurfs für den Datenschutzstandard ISPPPI, dass die darin vorgesehene Zustimmung schon den Erfordernissen nach Art. 2 DS-RL nicht entsprechen könne: „Aufgrund der Sanktionen und Konsequenzen, die verhängt werden können, wenn sich ein Teilnehmer weigert, den Verpflichtungen des Codes (zum Beispiel der Übermittlung von Daten über den Aufenthaltsort und die Erreichbarkeit) nachzukommen, gelangt die Arbeitsgruppe zu dem Schluss, dass die Zustimmung keineswegs ohne Zwang gegeben wird.“[92]

2.3. Gesetzliche Regelung als Rechtsgrundlage

Die Schaffung einer Rechtsgrundlage ist eine explizite, im WADC ausgedrückte (obwohl rechtlich irrelevante) „Erwartung“ der WADA *Stakeholder*, d. h. der SGBs[93]. Ferner (und wesentlicher) stellt nach Art. 49 Abs. 4 DSGVO („Ausnahmen für bestimmte Fälle“), (lit. d) („wichtige Gründen des öffentlichen Interesses“) die Voraussetzung einer Inanspruchnahme des EG 112 DSGVO dar. Nur ein Gesetz kann ein öffentliches Interesse, das auch nach deutschem Recht ein „qualifiziertes“[94] zu sein hat, nachweisen: „Vage Hinweise auf öffentliche Belange reichen nicht aus“, wobei der Nachweis durch die NADO zu erbringen ist.[95] Das AntiDopG kommt somit sowohl der WADA als auch den Aufsichtsbehörden potentiell entgegen.

2.3.1. §§ 8-10 AntiDopG: Möglichkeiten und Grenzen

Seit dem 01.01.2016 dient das Anti-Doping-Gesetz (AntiDopG) der Dopingbekämpfung zum Schutz von Gesundheit, Fairness, Chancengleichheit und der Integrität des Sports (§ 1). Unter Strafe stellt es die Herstellung, den Handel, den Vertrieb und die Verschreibung von in der Anlage I zum UNESCO-Übereinkommen genannten Dopingmitteln bzw. -methoden (§ 2) ebenso wie das so genannte Selbstdoping (§ 3). Zudem bieten §§ 8-10 AntiDopG eine explizite Rechtsgrundlage für die Datenübermittlung auch in Drittländer – eine Erneuerung, die *Wedde* 2011 als dringend eingestuft hatte.[96] Als Rechtsgrundlage entspricht es somit dem datenschutzrechtlichen Bestimmtheitsgrundsatz, ob es *per se* aber auch dem Grundsatz der Datensparsamkeit[97] entspricht, erscheint klärungsbedürftig. Dem Text sind keine direkt begrenzenden Normen zu entnehmen, so dass einem „collect-it-all-approach“ à la NSA[98] nichts im Wege steht. Beim EuGH-Urteil *Digital Rights Ireland* reichte dem Gericht die Abwesenheit einer solchen Begrenzung, um einen Grundrechtseingriff „von großem Ausmaß und von besonderer Schwere“ festzustellen[99] und die Richtlinie zur Vorratsspeicherung (RL 2006/24/EG)[100] für ungültig zu erklären.

Gerichte und Staatsanwaltschaften können auf Grundlage des AntiDopG der NADA „personenbezogene Daten aus Strafverfahren von Amts wegen übermitteln, soweit dies aus Sicht der übermittelnden Stelle für disziplinarrechtliche Maßnahmen im Rahmen des Dopingkontrollsystems der [NADA] erforderlich ist und ein schutzwürdiges Interesse der von der Übermittlung betroffenen Person nicht entgegensteht“ (§ 8); und die NADA ihrerseits darf Daten „erheben“, „verarbeiten“ und „nutzen, soweit dies zur Durchführung ihres Dopingkontrollsystems erforderlich ist“ (§ 9), einschließlich Gesundheitsdaten, bei denen jedoch Einschränkungen gelten (§ 10 Abs. 1). „Ergebnisse von Dopingproben und Disziplinarverfahren im Rahmen des Dopingkontrollsystems sowie eine erteilte medizinische Ausnahmegenehmigung“ darf die NADA einer anderen NADO, einem internationalen Sportfachverband, einem internationalen Veranstalter oder der WADA „übermitteln, soweit dieser oder diese für die Dopingbekämpfung nach dem Dopingkontrollsystem der [NADA] und der [WADA] zuständig ist und die Übermittlung zur Durchführung dieses Dopingkontrollsystems erforderlich ist“ (§ 10 Abs. 2).

Als gesetzliche Regelung i. S. v. Art. 42 Abs. 2 DSGVO stellt die durch §§ 8-10 AntiDopG bereitgestellte Regelung internationaler Datenübermittlungen durch die NADA auf eine scheinbar solide, wenn auch grundsätzlich anfechtbare Grundlage, *sofern* bis dahin die Bearbeitung rechtmäßig erfolgt war. Gemäß Art. 42 Abs. 2 DSGVO ist eine Einzelfallprüfung durch die Aufsichtsbehörden dann nicht erforderlich, was angesichts des vermutlich enormen Volumens der Datenströme[101] zu einer erheblichen Entlastung der Behörden führen dürfte. Dem Fallstrick eines „erheblichen Ungleichgewichts“ zwischen betroffener Person und verarbeitender Stelle (EG 34), der ansonsten objektiv auf das Anti-Doping-Arbeit Anwendung finden müsste, kann aufgrund der Anerkennung der Wahrung eines wichtigen öffentlichen Interesses nach Art. 44 Abs. 1 Lit. d) DS-GVO entkommen werden. Ob dann die *Athlete Consent Forms* aus den Sportanlagen verschwinden werden, bleibt freilich abzuwarten. Ungeklärt bleibt die Frage der weiteren Datenübermittlung von Kanada aus (*onward transfers*): Da Deutschland Kanada im Hinblick auf das dortige Schutzniveau vertraut, dürfen Daten nicht ohne weiteres von Kanada aus weiter übermittelt werden. Jedoch scheint ADAMS gerade für weltweiten Datenaustausch konzipiert zu sein, die WADA versteht sich selbst ausdrücklich als *central clearinghouse*[102], also quasi als Schaltstelle. Ebenso wie die kartellrechtliche Zulässigkeit von Anti-Doping-Regelungen davon abhängen, dass „sie auf das zum ordnungsgemäßen Funktio-

nieren des sportlichen Wettkampfs Notwendige begrenzt sind“[103], muss auch die Anti-Doping-Datenverarbeitung weiterhin den Maßstäben der Notwendigkeit und der Verhältnismäßigkeit genügen, genauso wie das neue Europaratsabkommen zur Spielmanipulation explizite Grundrechts- und Datenschutzvorbehalte beinhaltet.[104]

Die Frage nach der Rechtsgrundlage der Datenübermittlung an (vermutlich deutsche?) Strafverfolgungsbehörden wurde vom Bundesrat[105] im Rahmen einer Frage des Bundestags zum Gesetzentwurf an die Bundesregierung gestellt. Der Bundesrat begrüßte ausdrücklich die im Referentenentwurf vorgesehene gesetzliche Regelung, monierte jedoch, dass in § 8 AntiDopG-E nur die Übermittlung Strafverfolgungsbehörden → NADA, nicht aber umgekehrt NADA → Strafverfolgungsbehörden, geregelt sei. „Angesichts der in § 10 Absatz 2 AntiDopG-E ausdrücklich benannten möglichen Empfänger der gesundheitsbezogenen Daten – die Strafverfolgungsbehörden sind hier nicht aufgeführt – dürfte nach dem Gesetzesentwurf die Datenübermittlung an die Strafverfolgungsbehörden rechtlich fragwürdig sein.“[106] Die Bundesregierung indes fand in ihrer Antwort an den Bundestag die von ihr vorgeschlagene Regelung mehr als ausreichend.[107] „Die Bundesregierung hat die vom Bundesrat erbetene Prüfung vorgenommen. Eine gesetzliche Regelung zur Datenübermittlung von der [NADA] an die Strafverfolgungsbehörden ist aus der Sicht der Bundesregierung nicht angezeigt. Mit der Übermittlungsvorschrift des § 8 AntiDopG wird das Anliegen verfolgt, die Arbeit der NADA zu unterstützen. Eine spezielle gesetzliche Regelung für die Datenübermittlung von der NADA an die Strafverfolgungsbehörden ist nicht erforderlich. Im Übrigen wird auf Nummer 257a der Richtlinien für das Strafverfahren und das Bußgeldverfahren hingewiesen. Hiernach kann es für Gerichte und Staatsanwaltschaften im Ermittlungsverfahren, die Dopingstraftaten zum Gegenstand haben und einen Bezug zu Leistungssportlern bzw. deren Ärzten, Trainern, Betreuern oder Funktionären aufweisen, zweckmäßig sein, mit der NADA in Verbindung zu treten, die gegebenenfalls sachdienliche Auskünfte erteilen kann. Darüber hinaus enthält Art. 14.2 des Nationalen Anti-Doping Codes von 2015 bereits eine Verpflichtung der NADA zur umfassenden Zusammenarbeit mit den staatlichen Ermittlungsbehörden.“[108] Der Verweis auf Sachdienlichkeit erscheint datenschutzrechtlich wenig hilfreich.

Der Bundesregierung ist wohl einzuräumen, dass auf nationaler Ebene Datenübermittlungen von bzw. an die Strafverfolgungsbehörden auf jeden Fall rechtlich abgesichert werden können. Wenn aber Datenübermittlungen ins (insbesondere nichteuropäische) Ausland stattfinden, und die Empfänger keine Strafverfolgungsbehörden sind, ist dem Bundestag zuzustimmen, dass der Wortlaut im Hinblick auf diese Datenübermittlung keine spezifische Regelung bietet. Der Hinweis der Bundesregierung auf „die besonderen Schutzvorschriften der §§ 4b und 4c BDSG“[109] müsste eigentlich zur Unterbindung solcher Transfers führen können. Dass dies auch dazu führen könnte, dass die NADA den Erwartungen von WADA und *Stakeholders* nicht immer wird entsprechen können, gab die Bundesregierung zu: „Die NADA wird ihre Möglichkeiten nutzen, damit dem Schutz von Gesundheitsdaten bei der Übermittlung an Verbände und Veranstalter mit Sitz im Ausland Rechnung getragen wird, ohne dass dabei die Vorgaben des WADC verletzt werden. Dies kann z. B. dadurch erfolgen, dass die NADA besonders sensible Kategorien von Gesundheitsdaten nicht im automatisierten Datenverarbeitungssystem der WADA speichert, sondern lediglich auf der Basis bilateraler Vereinbarungen mit dem jeweiligen Verband oder Veranstalter mit Sitz im Ausland an diese übermittelt.“[110]

2.3.2. §§ 8-10 AntiDopG: Kritik der Datenschutzbeauftragten der Länder Rheinland-Pfalz und Schleswig-Holstein

In der Tat hatten die LfD RP u. SH zum damaligen Referentenentwurf eine Stellungnahme abgegeben, in der § 8 einer harten Kritik unterzogen wurde.[111] Moniert wurde u. a., dass dem NADA-Dopingkontrollsystem durch dynamische Verweisung auf „disziplinarrechtliche Maßnahmen“ ein „normativer Charakter verliehen“ und dadurch „eine hochsensible Datenübermittlung aus dem sanktionierenden hoheitlichen und den privaten Bereich“ erlaubt werde, ohne dass ausreichende „verfahrensrechtliche Sicherungen“ im Entwurf vorliegen würden.[112] Die Regelung zur Übermittlung durch Gerichte und Staatsanwaltschaften an die NADA sei im Hinblick auf das damit verfolgte schutzwürdige Interesse nicht hinreichend konkretisiert. Betroffene Athleten seien über solche Verfahren zu informieren, denn „Geheimverfahren“ seien „inakzeptabel“[113], was wahrscheinlich viele Insider der Anti-Doping-Community überraschen würde. Im WADA-Regelwerk zielen mehrere Bestimmungen des WADC[114] bzw. des ISTI[115] auf „Ermittlungen“ (*investigations*) bzw. auf „Nachrichten“ (*intelligence*) ab. Verschwiegenheit wird dabei kategorisch vorausgesetzt.[116]

Dem Umstand solcher Erwartungen kann Rechnung getragen werden, z. B. indem eine NADO (wie die dänische NADO, *Anti Doping Danmark*) als öffentlich-rechtliche Einrichtung (*selvejende Institution*) im Amtsbereich des (sportpolitisch zuständigen) Kulturministeriums definiert[117], oder indem (wie bei der britischen NADO) die durch die NADO betriebene Datenübermittlung durch eine vom Innenminister (*Home Secretary*) erlassene Verordnung (*Statutory Instrument*) explizit dem Datenaustausch der Strafverfolgungsbehörde SOCA (*Serious Organised Crime Agency*)[118] gemäß den Bestimmungen des nationalen Datenschutzrechts gleichgestellt wird, solange die Arbeit der britischen NADO (*United Kingdom Anti-Doping Limited, UKAD*) vom Innenminister als „im öffentlichen Interesse“ erachtet wird.[119] Dabei betonen die LfD RP u. SH in ihrer Stellungnahme, dass die NADA „keine ‚quasi-staatliche‘ Stelle [ist], der hoch sensible Informationen aus laufenden Ermittlungs- und Strafverfahren ungefiltert anvertraut werden dürften“ und ziehen deshalb das aus Anti-Doping-Sicht sicherlich unerfreuliche Fazit: „Eine Weitergabe von personenbezogenen Informationen an die außerstaatliche Stelle NADA vor einer vollständigen Information und Stellungnahmemöglichkeit des betroffenen Athleten erscheint ausgeschlossen.“[120] Moniert wird ferner, dass für den Informationstransfer von der NADA an die

Strafverfolgungsbehörden keine gesonderte Regelung vorgesehen war (und ist). „Dies ist deshalb verwunderlich, da ein Interesse etwa der Staatsanwaltschaft an Angaben aus dem ADAMS-Meldesystem („sog. Whereabouts") offensichtlich ist", weshalb der Gesetzgeber gefordert sei, eine eingehendere Regelung im Hinblick auf „Übermittlungs-, Beschlagnahme- oder Beweisverwertungsverbote oder -einschränkungen" zu treffen.[121]

Im Hinblick auf die für die vorliegende Untersuchung wichtige Übermittlung ins nichteuropäische Ausland verlangen LfD RP u. SH klare gesetzliche Vorgaben zu den Verwendungszwecken der von staatlichen Stellen an die NADA übermittelten Daten[122] im Hinblick auf die Weitervermittlung der Daten „an inner- und außereuropäische Empfänger (Verbände, Wettkampfveranstalter, Presse)".[123] Dass das AntiDopG dem Entwurf nach explizit darauf abzielt, die Weitervermittlung der Daten an SGBs, WADA und Veranstalter zu ermöglichen, rechtfertigt nach Meinung der Autoren der Stellungnahme keine Ausnahmeregelung, da die Daten besonders sensibel seien und die Übermittlung „von keinerlei Erforderlichkeitsprüfung abhängig gemacht wird. Allein die verbandliche ‚Zuständigkeit' des Datenempfängers soll als Legitimation für Datenweitergaben sogar ins außereuropäische Ausland ausreichen. Dies würde einen massiven Bruch mit Datenschutzgrundsätzen (vgl. §§ 4b und 4c BDSG) darstellen."[124] Dass der deutsche Bundesgesetzgeber durch das AntiDopG versucht hat, den (nicht rechtlich verbindlichen) internationalen sportpolitischen Verpflichtungen der NADA Rechnung zu tragen, davon bleiben die Autoren der Stellungnahme unbeeindruckt: „Bleiben Zweifel, so ist die Datenweitergabe zu unterlassen. Dies gilt auch dann, wenn sportinterne Regelungen wie der WADA Code anderes vorsehen. Das nationale Recht muss sich gegen internationale Absprachen zwischen Sportverbänden behaupten und durchsetzen."[125]

2.3.3. Erwägungsgrund 112 (EG 112) DSGVO: Möglichkeiten und Grenzen

Die WADA[126] und einige SGBs[127] hatten schon früh erkannt, dass die bisweilen als *gold standard* apostrophierte[128] DSGVO die Anti-Doping-Arbeit behindern könnte und versuchten daher bald, den EU-Gesetzgebungsprozess zugunsten von Bereichsausnahmen zu beeinflussen.[129] Vor diesem Hintergrund ist wohl der Wortlaut von EG 112 DSGVO zu verstehen, die Ausnahmen „insbesondere" für Datenübermittlungen zulässt, „die aus wichtigen Gründen des öffentlichen Interesses erforderlich sind, beispielsweise für den internationalen Datenaustausch zwischen Wettbewerbs-, Steuer- oder Zollbehörden, [...] und/oder Beseitigung des Dopings im Sport." Dass Dopingbekämpfung ungeachtet ihrer nationalen Rechtsgrundlage (d.h., auch wenn kein nationales Strafrecht Anwendung findet und die NADO keine Behörde ist) hier neben staatlichen Behörden, die staatliche Kernaufgaben wahrnehmen (Finanzen, Seuchenschutz, etc.), erwähnt wird, darf durchaus als Etappensieg von WADA und SGBs angesehen werden, bedarf jedoch einer näheren rechtlichen Überprüfung. EG 112 DSGVO lässt Ausnahmen zwar zu, welche durch nationale Aufsichtsbehörden zu erteilen sind, garantiert diese jedoch nicht (vgl. EG 111 und Art. 44). Vielmehr muss eine Rechtsgüterabwägung vorgenommen werden, die in der DSGVO explizit vorgesehen ist: „Das Recht auf Schutz der personenbezogenen Daten ist kein uneingeschränktes Recht; es muss im Hinblick auf seine gesellschaftliche Funktion gesehen und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden" (DSGVO, EG 4)[130], insbesondere gegen die Informationsfreiheit.[131] Die jüngste EuGH-Rechtsprechung hat die Rechte der von der Verarbeitung betroffenen Personen gestärkt[132] und die nationalen Aufsichtsbehörden nicht nur gefördert, sondern auch gefordert: Klagen sind aufzunehmen und bei entsprechender Rechtslage sind Schritte gegen die verarbeitenden Stellen zu nehmen.[133] Das Grundrecht auf rechtliches Gehör (Art. 47 EU-Grundrechtscharta) bedeutet, dass jedem Grundrecht ein wirksamer Rechtsbehelf gegenüberstehen muss, weshalb das englische High Court im Urteil *Vidall-Hall* die bisherige Rechtsprechung verwarf, die bei Verletzungen des Rechts auf Datenschutz bislang einen Rechtsbehelf nur bei nachgewiesenem monetärem Schaden aufgrund einer rechtswidrigen Handlung (*tort*) zugelassen hatte.[134] Anders als bei der Rechtsgüterabwägung zwischen Datenschutz und Informationsfreiheit freilich steht dem Datenschutz hier *kein* konkurrierendes Grundrecht entgegen. Das von der WADA postulierte „fundamental right to participate in doping-free sport"[135] ist ein reines WADA-Postulat.

Bei der Rechtsgüterabwägung zwischen Datenschutz und Informationsfreiheit kann ferner kaum größeres Entgegenkommen erwartet werden als z. B. bei der Überwachung elektronischer Kommunikation zu nachrichtendienstlichen und nationalen Sicherheitszwecken. Dort wollte jüngst die WP29 selbst bei expliziten vertraglichen oder auch gesetzlichen Regelungen eine Beeinträchtigung des Schutzniveaus nicht hinnehmen.[136] Als Ergebnis des *Schrems*-Urteils verkündete sodann die WP29 aufgrund einer umfassenden Analyse der Rechtsprechung von EuGH sowie EGMR „four European Essential Guarantees", die bei der Datenübermittlung in Drittländer zu beachten seien (präzise Bestimmungen; Nachweispflicht des legitimen Ziels, der Notwendigkeit und der Verhältnismäßigkeit; unabhängige Aufsicht; effektive Rechtsbehelfe)[137] und erteilte dem üblichen Pragmatismus ein deutliche Absage: „The Guarantees are based on what is required by the law and not necessarily on what is the current practice in the EU Member States".[138] EG 112 DSGVO soll in diesem Rahmen nicht weiter untersucht werden, stellt jedoch ein ganz eigenes Thema dar.[139]

2.3.4. Datenübermittlungen durch andere Organisationen bzw. Behörden als die NADA Deutschland

In dieser Untersuchung wurde die Frage der Rechtsgrundlage bei der Übermittlung anderer in Deutschland tätigen Organisationen als die NADA Deutschland bewusst ausgeklammert. Anti-Doping-Aktivitäten werden weiterhin nicht nur durch NADOs, sondern ebenfalls durch internationale Verbände[140] und Wettbewerbsveranstalter durchgeführt, die ggf. im Rahmen von *Outsourcing* private Firmen beauftragen können. Anders als die NADOs mancher anderer EU-Staaten ist die NADA Deutschland keine öffentliche Behörde, sondern eine privatrechtliche Stiftung, weshalb die datenschutzrecht-

liche Anerkennung ihrer Aufgaben durch das AntiDopG von großer Bedeutung ist. Bei den Anti-Doping-Aktivitäten anderer Organisationen ist davon auszugehen, dass die fragwürdige Athleteneinwilligung weiterhin als Rechtsgrundlage verwendet wird. Sofern die NADA Deutschland mit Organisationen im In- und Ausland Daten austauscht, kann sie durch rechtlich verbindliche Abkommen ihre Partner zur Einhaltung datenschutzrechtlicher Grundsätze verpflichten, z. B. ist ein zwischen der NADA und ihrer britischen Schwesterorganisation UK Anti Doping (UKAD) unterzeichnetes Datenaustausch-Abkommen[141] bekannt. Andere Organisationen können ebenfalls vertraglich das Risiko auf rechtswidrige Verarbeitung reduzieren.

Ebenfalls ausgeklammert wurde die Datenübermittlung durch Strafverfolgungsbehörden (Polizei, Zoll, Staatsanwaltschaft, etc.), für die eigenständige Regelwerke gelten – die EU-weiten Vorgaben der RL (EU) 2016/680[142] über Strafverfolgungsbehörden allgemein sowie insbesondere der RL (EU) 2016/681[143] zur Verwendung von Fluggastdatensätzen (PNR-Daten) sind durch nationale Vorschriften umzusetzen und ggf. zu konkretisieren, welche verglichen mit dem Datenaustausch durch privatrechtliche Organisationen für einen reibungslosen Ablauf wahrscheinlich vorteilhafter sind. Doch auch Strafverfolgungsbehörden werden durch Aufsichtsbehörden des Datenschutzes vermehrt in die Pflicht genommen, was das Beispiel des EuGH-Urteils zur Vorratsspeicherung[144] ebenso wie das Urteil des Bundesverfassungsgerichts zum BKA-Gesetz[145] verdeutlichen. Selbst beim hochsensiblen Schengener Informationssystem (SIS II) muss sichergestellt werden, dass die betroffenen Personen ihre Rechte ausüben können.[146] Auf jeden Fall kann jedoch – sehr vorteilhaft – bei Strafverfolgungsbehörden die Frage des öffentlichen Interesses unzweifelhaft bejaht werden.

3. Fazit

3.1. Datenschutzrechtliches und rechtspolitisches Fazit

Diese Untersuchung hat gezeigt, dass das AntiDopG ein Gesetz zur rechten Zeit war, da erst durch dessen §§ 8-10 eine explizite (wenn auch nicht zwangsläufig einwandfreie) Rechtsgrundlage der Datenübermittlungen ins nichteuropäische Ausland geschaffen wurde. Der von WADA und EOC erwirkte EG 112 DSGVO bietet nur teilweise Abhilfe, da zuvor die Erhebung der Daten rechtmäßig gewesen sein muss und nur dann, wenn ein Gesetz vorliegt. Weder die Übereinkommen von Europarat und UNESCO, noch Art. 165 AEUV ändern hieran etwas. Die Vorteile einer gesetzlichen Regelung sind offenkundig, denn die traditionsreichen Arrangements aufgrund einer stets angreifbaren Athleteneinwilligung bleiben wackelig. Ob dafür die Nachhaltigkeit des AntiDopG als gegeben angesehen werden kann, kann freilich derzeit nicht bestätigt werden. Ob das AntiDopG den strafrechtlichen bzw. rechtspolitischen Grundsätzen von Notwendigkeit und Verhältnismäßigkeit entspricht, wurde im Rahmen einer Anhörung von Rechtslehren durch einige Teilnehmer bezweifelt, noch bevor die Vorlage vom Bundestag verhandelt wurde[147]. Gerade die datenschutzrechtlichen Aspekte wurden zwei Monate vor der Verabschiedung durch den Bundestag unisono von einem Verfassungsrichter a. D., Udo *Steiner*, und durch Stefan *Brink* vom LfD Rheinland-Pfalz (RP) bemängelt („keine klaren Vorgaben“)[148]. Wiederholt wurden diese Bedenken von *Lehner*[149], der auch weitere verfassungsrechtliche Probleme (Schiedszwang, Doppelbestrafung) identifizierte, und im März 2016 zeichnete sich die Möglichkeit einer Verfassungsklage ab.[150] In einem offenen Brief an DOSB-Präsident Alfons Hörmann vom 23.02.2015 bezeichneten Sylvia *Schenk* (Rechtsanwältin, ehemalige Radfahrerpräsidentin und Sportexpertin von Transparency International) und Stefan *Brink* (LfD RP) das Anti-Doping-Gesetz als „grandioses Ablenkungsmanöver“. Die anschließende Kritik fiel gerade bei datenschutzrechtlichen Aspekten des AntiDopG vernichtend aus. Angeprangert wurden potentielle Interessenskonflikte in den NADA- und NADA-nahen Entscheidungsgremien („Das positive Beispiel an der Spitze“), u. a. da das Bundesministerium des Inneren (BMI) gleichzeitig für eine am olympischen Medaillenspiegel orientierte Sportförderung des Bundes sowie für die deutsche Anti-Doping-Politik zuständig ist („Das BMI hat ein Rechtsstaatsproblem“). Grundsätzlich in Frage gestellt wurde der aktuelle (von WADA, IOC und SGBs befürwortete) Zugang zu Anti-Doping, der durch eine Abwesenheit von Verhältnismäßigkeit gekennzeichnet sei: „Der DOSB darf aber nicht schweigen, er muss Fürsprecher sein. Gerade wenn es darum geht, die Belastungen des Anti-Doping-Systems grundrechts- und athletenfreundlich abzumildern. Gemeinsam mit der NADA könnte er nach datenschutzfreundlichen Alternativen im Anti-Doping-Kampf suchen. Ist es wirklich zwingend notwendig, dass Spitzensportler im Vorhinein detaillierte Angaben über Aufenthaltsorte, Erreichbarkeit und Medikation auf einem Server in Kanada hinterlegen müssen, dessen Sicherheit und Zugriffsberechtigungen nicht kontrolliert werden können? Lassen sich stattdessen nicht weniger eingriffsintensive Verfahren wie eine freiwillige Ortung des Smartphones im Kontrollfall entwickeln? Und kann man nicht vollständig auf pauschale Datenübermittlungen insbesondere von sensiblen Gesundheitsdaten ins außereuropäische Ausland verzichten?“ Kritisiert wurden ferner die Abwesenheit eines deutschen Datenservers (alle Daten werden in Kanada gespeichert), einer NADA-Beschwerdestelle für Athleten, einer Positivliste unbedenklicher Nahrungsergänzungsmittel (wobei einige Olympiastützpunkte durch Werbung für ggf. von der NADA nicht empfohlene Nahrungsergänzungsmittel finanziert würden) ebenso wie Alternativen zur Sichtkontrolle bei der Urinabgabe.[151]

Zuvor hatten die LfD RP und SH, wie bereits dargestellt, beim Referentenentwurf erhebliche Mängel festgestellt. Er sei „insoweit zu begrüßen, als er den Schutz informationeller Selbstbestimmung als Regelungsmaterie ausdrücklich benennt und erste Regelungsvorschläge macht. Allerdings bestehen erhebliche Zweifel daran, dass der Entwurf mit Blick auf das informationelle Selbstbestimmungsgrundrecht der Sportlerinnen und Sportler den verfassungsrechtlichen Anforderungen des Wesentlichkeitsgrundsatzes und der Normbestimmtheit sowie den bestehenden staatlichen Schutzpflichten zugunsten der Athleten gerecht wird. Hier sind substanzielle Ergänzungen und Konkre-

tisierung schon auf gesetzlicher Ebene geboten."[152] Ähnlich hatte es der sehr sportkundige Verfassungsrichter a. D. Udo *Steiner* gesehen.[153]

Die gesetzliche Regelung bleibt die mit Abstand beste Lösung, sofern das betreffende Gesetz aufrechtzuerhalten ist. Dass das AntiDopG möglicherweise gar nicht so sehr geschaffen worden ist, um datenschutzrechtliche Lücken zu schließen, sondern vielmehr als flankierende Maßnahme einer (mittlerweile zurückgezogenen) deutschen Olympiabewerbung entstanden sein könnte[154], ändert an diesem Befund nichts. Eine Übermittlung aufgrund Einwilligung kann stets angefochten werden, und dass am 07.06.2016 der BGH im Fall *Pechstein* die Wirksamkeit von Schiedsvereinbarungen bestätigt hat, da eine kartellrechtlich begründete Unwirksamkeit nach Art. 102 AEUV nicht festgestellt werden könne[155] und der „unfreiwillige Verzicht auf die Grundrechtsausübung" weder durch „physische oder psychische Gewalt, z. B. durch Drohung mit einem empfindlichen Übel" erwirkt worden sei[156], lässt im Übrigen keinen analogen Schluss über Anti-Doping-Datenverarbeitungs-Vereinbarungen zu, da im Datenschutz besondere, etablierte Maßstäbe zur Beurteilung einer freien und informierten Zustimmung bestehen. Die anscheinend kartellrechtlich unproblematische, vom BGH selbst als fremdbestimmt eingestufte[157] Einwilligung würde einer datenschutzrechtlichen Prüfung wohl nicht standhalten.

Der datenschutzrechtliche Rechtmäßigkeitsvorbehalt, die Grundsätze von Notwendigkeit und Verhältnismäßigkeit sowie der Status dieser Normen als Grundrechte sind für den europäischen Datenschutzbegriff, anders als in den USA, Australien oder China[158], geradezu konstitutiv. Das europäische Modell mag anderen altmodisch bis paternalistisch erscheinen[159], verhandelbar ist es aber nicht. Akteure in Sport und Anti-Doping mögen zwar den Eindruck haben, als sei der US-Ansatz verbreiteter, dabei verkennen sie jedoch, dass im Jahr 2012 weltweit mehr Länder bei der Verabschiedung neuer Gesetze dem europäischen als dem US-Ansatz gefolgt waren,[160] wobei die USA und China (nach *Greenleaf: significant outliers*) eher isoliert sind.[161] Vor diesem Hintergrund ist es nachvollziehbar, dass die EU im Rahmen der Revision des WADC 2009 besonders auf Einhaltung ihrer Datenschutznormen beharrte[162], die durch den Übergang von der DS-RL zur DSGVO merkbar gestärkt werden. Dass die effektive Umsetzung dieser Normen (*enforcement*) weiterhin Probleme bereiten kann[163] und die erstrebte extraterritoriale Wirkung[164], egal ob rechtsdogmatisch vertretbar[165], *de facto* davon abhängt, ändert an den grundsätzlichen Rechtspositionen nichts. Es geht um digitale Souveränität.[166] Ob dabei NADOs den Nachweis der Notwendigkeit und Verhältnismäßigkeit werden erbringen können, hängt von der Fähigkeit des gesamten Anti-Doping-Systems, den Umfang des Phänomens Doping und die Effekte der Bekämpfung nachzuweisen, ganz entscheidend ab.[167] Empirisch-sportwissenschaftliche Beiträge dürften auch rechtlich relevant sein. Wenn z. B. der Anti-Doping-Kampf auf einer impliziten „Abschreckungstheorie" (*deterrence theory*) baut[168], bedarf es empirischer Evidenz der gemachten Fortschritte, um die Notwendigkeit und Verhältnismäßigkeit der ergriffenen Maßnahmen rechtlich würdigen zu können. Bei der Annahme, durch diese Maßnahmen ein unterstellt exzessives Verhalten kontrollieren zu können, wird vielleicht übersehen, dass Spitzensport an sich ein exzessives Handlungssystem darstellt.[169]

3.2. Sportrechtliches und sportpolitisches Fazit

Datenschutzrechtlich liegt an sich wenig Neues vor, es sei denn die Einsicht, dass auch im Sport umfassende Datenverarbeitungsvorgänge die Aufmerksamkeit der Aufsichtsbehörden verlangen und dass die betroffenen Personen (auch) hier (sei es aus Unwissen, aus Angst vor Repressalien oder aufgrund freier, informierter Zustimmung) wenig unternehmen, um ihr Grundrecht auf Datenschutz geltend zu machen. Sportrechtlich und sportpolitisch dagegen zeigt die Untersuchung ein neues Beispiel von Konfliktpotential zwischen staatlichem Recht und *lex sportiva*. Von Aufsichtsbehörden ist wenig Flexibilität zu erwarten, zumal diese sich im Rahmen der WP29 zu einer strikten Auslegung der für die Übermittlung in Drittstaaten geltenden Beschränkungen verpflichtet haben.[170] Dass der Anti-Doping-Kampf bereits vielfach Begrenzungen der Freiheitsrechte von Athleten beinhaltet[171], muss Aufsichtsbehörden des Datenschutzes nicht zwangsläufig überzeugen.

Die Auslegung dieser Vorschriften wird auch nicht zuletzt von der allgemeinen sportpolitischen und sportrechtlichen Entwicklung abhängen und insbesondere von der Bereitschaft staatlicher Gerichte, Normen der *lex sportiva* als Schranken der staatlichen Normen anzuerkennen. Unionsrechtlich betrachtet, stellen die hier untersuchten Probleme einen geradezu klassischen Fall der „indirekten Sportpolitik"[172] der EU dar: Wie das Freizügigkeitsrecht im *Bosman*-Urteil[173] greifen auch hier sportfremde EU-Normen in das sportliche, sportrechtliche und sportpolitische Geschehen ein. Das (aus hiesiger Sicht nicht nachvollziehbare) Entgegenkommen des BGH im *Pechstein*-Urteil durch die Feststellung, SGBs und Athleten würden sich bei der Bekämpfung des Dopings grundsätzlich nicht als von gegensätzlichen Interessen geleitete „Lager" gegenüber stehen[174], wäre ein solches Beispiel, muss aber dafür nicht Schule machen. Besorgniserregend erscheint jedoch bisweilen die lockere Einstellung von WADA und SGBs zum Rechtmäßigkeitsvorbehalt des Datenschutzrechts. Im Vorfeld der XXII. Olympischen Winterspiele in Sotschi (2014) wurde z. B. bekannt, dass das IOC von allen teilnehmenden Nationen die Anwendung der ADAMS-Datenbank erwartete[175], obwohl sich dies für Teilnehmer aus der EU als potentiell rechtswidrig erwies. Während das Europäische Parlament[176] sich über die Rolle russischer Geheimdienste in Sotschi besorgt zeigte, erkannte auch die WADA selbst (18 Monate vor Sotschi), dass das IOC-Reglement für Teilnehmer aus der EU durchaus zu Datenschutzrechtsverletzungen führen könnte, zeigte sich darüber aber nicht weiter besorgt.[177] Also fragte eine internationale Sportlergewerkschaft, ob die WADA-Führung wissentlich zum Gesetzesbruch aufgefordert habe.[178] Das Beispiel verdeutlicht, dass der Sport einer kritischen, informierten Diskussion zum Privat-

lebens- und Datenschutz bedarf. Dass dies zwei verschiedene Problemkreise sind[179], wird zu oft übersehen. Beaufsichtigtes Urinieren mag eine Privatlebensverletzung sein, stellt an sich aber keine Datenschutzverletzung dar. Wer aber das Anti-Doping-System kritisch kommentiert, hat einen schweren Stand, da das Thema Doping medienwirksam bearbeitet wird und NADOs sich weitreichenden Erwartungen von WADA und SGBs zu stellen haben.

1 Jacob Kornbeck, Ph.D., Obwohl der Verfasser EU-Beamter ist, kommen im vorliegenden Beitrag ausschließlich eigene Meinungen und keine amtlichen Positionen des EDPS bzw. der EU zum Ausdruck.

2 Kuner, Ch.: European Data Privacy Law and Online Business. Oxford: Oxford University Press (2003), S. 16.

3 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. ABl. EU L 281, 23.11.1995, S. 31–50.

4 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR). ABl. EU L 119, 04.05.2016, S. 1–88.

5 Deutscher Bundestag: Drucksache 18/4898. 13.05.2015. Gesetzentwurf der Bundesregierung. Entwurf eines Gesetzes zur Bekämpfung von Doping im Sport. (http://dip21.bundestag.de/dip21/btd/18/048/1804898.pdf), S. 36.

6 Anti-Doping-Gesetz (AntiDopG): Gesetz zur Bekämpfung von Doping im Sport vom 10.12.2015. BGBl. I, Nr. 5, 17.12.2015, S. 2210-2217.

7 WADA: World Anti-Doping Code 2015, https://www.wada-ama.org/en/what-we-do/the-code.

8 Mortsiefer, L.: Datenschutz im Anti-Doping-Kampf. Bonn 2011: Gardez., S. 243.

9 Prohibited Substances and Methods (“List”); International Standard for Testing and Investigations (“ISTI”); International Standard for Laboratories (“ISL”); International Standard for Therapeutic Use Exemptions (“ISTUE”); International Standard for the Protection of Privacy and Personal Information (“ISPPPI”), https://www.wada-ama.org/en/international-standards.

10 European Convention on Spectator Violence and Misbehaviour at Sports Events 1985. CETS No. 120 (http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/120) = Europäisches Übereinkommen über Gewalttätigkeiten und Fehlverhalten von Zuschauern bei Sportveranstaltungen und insbesondere bei Fußballspielen. Straßburg/Strasbourg, 19.VIII.1985 = Amtliche Übersetzung Österreichs (http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168007a0f4). Anti-Doping Convention 1989. CETS No. 135 (http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/135) = Übereinkommen gegen Doping. Straßburg/Strasbourg, 16.XI.1989 = Amtliche Übersetzung Deutschlands (http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168007b0f4). Convention on the Manipulation of Sports Competitions 2014. CETS No. 215 (http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/215) = Derzeit keine deutsche Übersetzung = Council of Europe Convention on the Manipulation of Sports Competitions. Magglingen/Macolin, 18.IX.2014 (z.Z. keine deutsche Übersetzung) (http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/09000016801cdd7e).

11 International Convention against Doping in Sport 2005. Paris, 19 October 2005, (http://portal.unesco.org/en/ev.php-URL_ID=31037&URL_DO=DO_TOPIC&URL_SECTION=201.html).

12 Vertragsparteien sind lediglich verpflichtet, die Prinzipien des Übereinkommens zu unterstützen (Art. 4 Abs. 1), indem sie geeignete Maßnahmen ergreifen (Art. 3 Abs. 1).

13 BGH: U. v. 07.062016 - KZR 6/15. Nr. 97/2016. ECLI:DE:BGH:2016:070616UKZR6.15.0 (Pechstein), Rn. 63.

14 Backhouse, S. et al.: Study on Doping Prevention: A map of Legal, Regulatory and Prevention Practice Provisions in EU 28. Luxembourg 2014: Publications Office of the European Union. http://ec.europa.eu/sport/news/2014/docs/doping-prevention-report_en.pdf; Houlihan, B./Garcia, B.: The use of legislation in relation to controlling the production, movement, importation, distribution and supply of performance-enhancing drugs in sport (PEDS). Loughborough University 2012: WADA-UNESCO, https://www.wada-ama.org/sites/default/files/resources/files/UNESCO-Legislative-Research-Report-FINAL.pdf; Parzeller, M./Prittwitz, C., et al.: Rechtsvergleich der strafrechtlichen Normen und der strafprozessualen Verfolgung des Dopings im Leistungs- und Spitzensport in Deutschland, Italien, Frankreich, Schweiz und Spanien. BISp-Jahrbuch 2009/10, 315-326 ; T.M.C. Asser Instituut: The implementation of the WADA Code in the European Union. Report commissioned by the Flemish Minister responsible for Sport in view of the Belgian Presidency of the European Union in the second half of 2010. The Hague 2010: T.M.C. Asser Instituut. http://www.asser.nl/upload/documents/9202010_100013rapport%20Asserstudie%20(Engels).pdf.

15 UNESCO Convention 2005 (a. a. O., Fn. 10), Art. 4 Abs. 2.

16 WADA: Comments to the Proposed EU Data Protection Regulation. Agenda Item # 5.1. Attachment 1. (undated WADA meeting table document) http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-DO%20-%20Item_5_1_Attach_1_WADA_Comments_to_DP_Regulation-EU_Presidency_FINAL.pdf.

17 Deutscher Bundestag: Wissenschaftliche Dienste: Das Dopingkontrollsystem in Deutschland. Rechtlich-regulative Grundlagen und Reformoptionen. WD 10 - 3000 - 084/14. 03.11.2014. (https://www.bundestag.de/blob/410226/aa21e92fbf398877cb19faedb2be1809/wd-10-084-14-pdf-data.pdf), S. 13, Fn. 24.

18 WADA: International Standard for the Protection of Privacy and Personal Information (ISPPPI), 2014, https://www.wada-ama.org/en/resources/data-protection/international-standard-for-the-protection-of-privacy-and-personal.

19 Stellungnahme 3/2008 zum Entwurf eines Internationalen Datenschutzstandards zum Welt-Anti-Doping-Code. Annahme am 01.08.2008. WP 156. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2008/wp156_de.pdf; Zweite Stellungnahme 4/2009 zum Internationalen Standard der Welt-Anti-Doping-Agentur (WADA) zum Schutz der Privatsphäre und personenbezogener Informationen, zu entsprechenden Vorschriften des WADA-Codes und zu anderen Datenschutzfragen im Bereich des Kampfes gegen Doping im Sportdurch die WADA und durch (nationale) Anti-Doping-Organisationen. Annahme am

06.042009. WP 162. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp162_de.pdf; 05.03.2013 Letter from the Article 29 Working Party addressed to World Anti-Doping Agency, regarding 3rd stage of WADA's consultation in the context of the review of the World Anti-Doping Code and its International Standards, http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130305_letter-to-wada_en.pdf; Contribution of the Article 29 Working Party to the 3rd stage of WADA's consultation in the context of the review of the World Anti-Doping Code and its International Standards – Ref. Ares(2013)289160 – 05/03/2013. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130305_letter-to-wada_annex_en.pdf; WP29: Stellungnahme 7/2014 zum Schutz personenbezogener Daten in Québec. Angenommen am 04.06.2014. 1443/15/DE. WP 219. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp219_de.pdf.

20 Waddington, I.: Surveillance and control in sport: a sociologist looks at the WADA whereabouts system. IJSPP, 2:3 (2010), 255-274.

21 EU Conference on Anti-Doping: Organised by the European Commission. Athens, Greece, 13 – 15 May 2009. Conclusions of the Conference. http://old.minedu.sk/data/USERDATAEN/Sport/AntiDoping/athens_conf_conclusions_final_version_en.pdf.

22 Ministry of Health, Welfare and Sport [The Netherlands]: Report on EU Anti-Doping Conference, 15 June 2016 in Amsterdam: „The fight against doping in the EU legal framework: balance between effective anti-doping measures and fundamental rights". Organised by the Ministry of Health, Welfare and Sport in the context of the EU Presidency of the Netherlands. http://auteurs.allesoversport.nl/wp-content/uploads/2016/06/Report-on-the-anti-doping-conference-15-June-2016-1.pdf.

23 Datenschutzbeauftragter Kanton Zürich: Videoüberwachung durch öffentliche Organe, 2002. Eidgenöss. Datenschutzbeauftragter (EDSB): Umgang mit Mitgliederdaten in einem Verein, 2003. Zit. Baeriswyl, B.: Datenschutzrecht und Sport. In: Arter, O./Baddeley, M. (Hrsg.): Sport und Recht. Bern 2006: Schulthess, 133-156.

24 Flueckiger, Ch.: Dopage, santé des sportifs professionnels et protection des données médicales. Genf 2008: Schulthess.

25 « Au travers de notre étude, des atteintes illicites à la personnalité causées spécifiquement par des traitements de données sont mises en lumière. » Flueckiger (2008) (a. a. O., Fn. 24), S. 307, Rn. 1164.

26 « Ces observations remettent en cause des pratiques bien établies dont quasiment personne ne s'était inquiété sous l'angle du droit de la protection des données des sportifs. » Flueckiger (2008) (a. a. O., Fn. 24), S. 307, Rn. 1165.

27 Flueckiger (2008) (a. a. O., Fn. 24), S. 307, Rn. 1165.

28 Flueckiger (2008) (a. a. O., Fn. 24), S. 310, Rn. 1175.

29 Flueckiger (2008) (a. a. O., Fn. 24), S. 82-84, Rn. 269-276.

30 Niewalda, J.: Dopingkontrollen im Konflikt mit allgemeinem Persönlichkeitsrecht und Datenschutz. Berlin 2011: Duncker & Humblodt.

31 Mortsiefer (2011) (a. a. O., Fn. 8).

32 Weichert, Th.: [Sammelrezension]. DANA, 4/2011, S. 166-167.

33 Neuendorf, S.: Datenschutzrechtliche Konflikte im Anti-Doping-System. Am Beispiel des Anti-Doping Administration and Management Systems ADAMS. (SchrSpR 35). Baden-Baden 2015: Nomos.

34 Neuendorf, S. (2015) (a. a. O., Fn. 33), S. 5: „Neben dem Gefühl einer permanenten Einschränkung meiner Bewegungsfreiheit und der Angst vor den gravierenden Folgen von Eingabefehlern für meine sportliche Laufbahn, kamen mir auch Zweifel an der datenschutzrechtlichen Konformität des Systems".

35 Neuendorf, S. (2015) (a. a. O., Fn. 33), S. 68.

36 Neuendorf, S. (2015) (a. a. O., Fn. 33), S. 188.

37 Ausnahme: Weichert, Th.: Die Fussball-WM als Überwachungs-Grossprojekt. DANA, 1/2005, S. 7 ff.

38 Landesbeauftragte für Datenschutz Rheinland Pfalz und Schleswig-Holstein: Positionspapier des Landesbeauftragten für den Datenschutz Rheinland Pfalz (LfD Rh.Pf.) und des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD). Mainz und Kiel, 26.07.2011. Datenschutz und Dopingbekämpfung, https://www.datenschutzzentrum.de/allgemein/20110726-positionspapier-dopingbekaempfung.html.

39 Weichert (2011) [Sammelrezension]. DANA, 4/2011, S. 166-167.

40 Niewalda (2011) (a. a. O., Fn. 30).

41 Wedde, P.: Rechtsgutachten zum Thema „Datenschutzrechtliche Bewertung der Melde- und Kontrollpflichten im Rahmen von Anti-Dopingprogrammen, die die von SP.IN vertretenen Athleten betreffen". Erstattet von Prof. Dr. Peter Wedde. Eppstein/Ts., 5. September 2011, http://www.spinbb.net/uploads/media/Wedde_-_Gutachten_fu__r_SP.IN_per_5.9.2011.pdf.

42 Palmer, W./Taylor, S./Wingate, A.: "Adverse Analyzing". A European Study of Anti Doping Organization Reporting Practices and the Efficacy of Drug Testing Athletes. Nyon: UNI Global Union, http://www.euathletes.org/wp-content/uploads/2016/11/Adverse_Analyzing__FINAL__02.pdf.

43 EU Athletes: 12. February 2013. 100,000 Elite Athletes Call for Fundamental Reform at WADA, http://www.euathletes.org/media-press/news-from-eu-athletes/eu-athletes-news/browse/5/article/100000-elite-athletes-call-for-fundamental-reform-at-wada/news.html?tx_ttnews%5BbackPid%5D=361&cHash=e10b6cd12687f37d79263c538221798c.

44 Schaar, P.: Anforderungen des Datenschutzes an Dopingkontrollen. Unveröff. Manuskript. (Email-Wechsel mit dem Autor). (undatiert). http://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/Tagungsbaende/TagungsbandBeitragDopingkontrolle.pdf?__blob=publicationFile&v=5.

45 Lambertz, P.: Problematische Namensveröffentlichungsregelung in Dopingfällen gemäss WADA-Code. CaS 4/2015, 369 ff.

46 Börding, A./Schönfeld, M. von: Big Data im Leistungssport – Datenschutzrechtliche Anforderungen an die Vereine. CaS, 1/2016:1, 7-12.

47 Plass, J./Giffeler, D.: Anti-Doping-Kontrollen mit „eves". DANA 4/2016, 158-161.

48 „Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden." Charta der Grundrechte der Europäischen Union. Abl. EU C 326, 26.10.2012, S. 391–407.

49 FRA [Agentur der Europäischen Union für Grundrechte] & Europarat: Handbuch zum europäischen Datenschutzrecht. Luxemburg 2014: Amt für

Veröffentlichungen der Europäischen Union, http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_de.pdf, S. 71.

50 Ph. Scholz/B. Sokol in Simitis, S. (Hrsg.): Bundesdatenschutzgesetz. Kommentar. 8. Aufl. Baden-Baden: Nomos 2014, § 4 Rn. 3 ff. m. w. N.

51 Gola, P./Klug, Ch./Körffer, B./Schomerus, R.: BDSG Bundesdatenschutzgesetz Kommentar. 12. Aufl. München 2015: C.H.Beck, § 4 Rn. 3 ff.. Zustimmend Sokol in Simitis (2014) (a. a. O., Fn. 50), § 4 Rn. 3 ff. m. w. N.

52 Gola/Klug/Körffer/Schomerus (2015) (a. a. O., Fn. 51), § 4 Rn. 3.

53 Taranto, L.: Data Protection Principles, in Ustaran, E.: European Privacy: Law and Practice for Data Protection Professionals. Portsmouth, NH 2012: IAPP, S. 83.

54 S. Simitis, in Simitis (2014) (a. a. O., Fn. 50), S. 415, Rn. 3.

55 Ph. Scholz/B. Sokol, in Simitis (2014) (a. a. O., Fn. 50), § 4 Rn. 12.

56 M. Kuschewsky, in Kuschewsky, K. (Hrsg.): Data Protection and Privacy – Jurisdictional Comparisons. 2nd edition. London 2014: Thomson Reuters, S. 161.

57 Greenleaf, G.: The influence of European data privacy standards outside Europe: implications for globalization of Convention 108. IDPL 2:2 (2012), 68-92.

58 S. Simitis, in Simitis (2014) (a. a. O., Fn. 50), S. 136, Rn. 149.

59 Blume, P.: EU adequacy decisions: the proposed new possibilities. IDPL, 5:1 (2015), 34-39, zit. 34.

60 Senécal, F.: La protection des données de santé des athlètes dans le cadre de la lutte contre le dopage. LE, 11:2 (2006), 1-23, zit.14.

61 EuGH: U. v. 15.12.1995. Rs. C-415/93. Union royale belge des sociétés de football association ASBL gegen Jean-Marc Bosman, Royal club liégeois SA gegen Jean-Marc Bosman und andere und Union des associations européennes de football (UEFA) gegen Jean-Marc Bosman. Slg. 1995 I-04921. ECLI:EU:C:1995:463. (Bosman).

62 Parensen, A.: Die Fußball-Bundesliga und das Bosman-Urteil. In: Tokarski, W. (Hrsg.): EU-Recht und Sport. Aachen 1998: Meyer & Meyer, 70-150.

63 WP29: Arbeitspapier über eine gemeinsame Auslegung des Art. 26 Absatz 1 der Richtlinie 95/46/EG vom 24.10.1995 u. v. 25.11.2005. WP 114. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp114_de.pdf, S. 15.

64 S. Simitis, in Simitis (2014) (a. a. O., Fn. 50), § 4c Rn. 17.

65 EuGH: U. v. 06.11.2003. Rs. C-101/01. Strafverfahren gegen Bodil Lindqvist. Slg. 2003 I-12971, ECLI:EU:C:2003:596 (Lindquist), vgl. E. Ustaran, in Ustaran (2012), S. 174-175.

66 Diese Bestimmung war bislang unter Art. 40 enthalten, wurde jedoch zwischen dem 15.12.2015 und dem 06.04.2016 in die Begründungserwägungen verlegt.

67 Siehe Übersicht: Commission decisions on the adequacy of the protection of personal data in third countries, http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

68 2000/520/EG: Entscheidung der Kommission vom 26.07.2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA (Bekannt gegeben unter Aktenzeichen K(2000) 2441) (Text von Bedeutung für den EWR.) Abl. Nr. L 215 vom 25.08.2000, S. 7-47.

69 S. Simitis, in Simitis (2014) (a. a. O., Fn. 50), § 4b Rn. 78.

70 EuGH: U. (Große Kammer) v. 06.10.2015. Rs. C-362/14. Maximillian Schrems gegen Data Protection Commissioner. ECLI:EU:C:2015:650 (Schrems).

71 „Die Kommission wird jetzt Konsequenzen aus dem Urteil ziehen und [...] solche Beschlüsse in Zukunft regelmäßig überprüfen.“ Siehe Europäische Kommission: Mitteilung der Kommission an das Europäische Parlament und den Rat zu der Übermittlung personenbezogener Daten aus der EU in die Vereinigten Staaten von Amerika auf der Grundlage der Richtlinie 95/46/EG nach dem Urteil des Gerichtshofs in der Rechtssache C-362/14 (Schrems). Brüssel, den 06.11.2015. COM(2015) 566 final, S. 15.

72 2002/2/EG: Entscheidung der Kommission vom 20.12.2001 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzes, den das kanadische Personal Information Protection and Electronic Documents Act bietet (Bekannt gegeben unter Aktenzeichen K(2001) 4539). ABl. Nr. L 002 v. 04.01.2002, S. 13-16.

73 Consolidation. Personal Information Protection and Electronic Documents Act. S.C. 2000, c. 5. Current to June 6, 2016. Last amended on June 23, 2015 (http://laws-lois.justice.gc.ca/PDF/P-8.6.pdf).

74 Second Session, Forty-first Parliament, 62-63-64 Elizabeth II, 2013-2014-2015. Statutes of Canada 2015 Chapter 36. An Act to implement certain provisions of the budget tabled in Parliament on April 21, 2015 and other measures. Assented to 23rd June, 2015. Bill C-59. Schedule 2 (Section 166) Schedule 4 (Subsection 4(1.1) and paragraph 26(2)(c)) (http://www.parl.gc.ca/content/hoc/Bills/412/Government/C-59/C-59_4/C-59_4.PDF), siehe S. 158: “Organizations”.

75 WP29: Statement of the Article 29 Working Party. Brussels, 16 October 2015. http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf.

76 Restoring trust in transatlantic data flows through strong safeguards: European Commission presents EU-U.S. Privacy Shield Brussels, 29 February 2016. Press release IP/16/433. http://europa.eu/rapid/press-release_IP-16-433_en.htm.

77 EDPS (European Data Protection Supervisor): Opinon 4/2016. Opinion on the EU-U.S. Privacy Shield draft adequacy decision. 30 May 2016. (https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-05-30_Privacy_Shield_EN.pdf).

78 Meyer, D.: Hamburg’s DPA aiming to challenge Privacy Shield. The Privacy Advisor, Aug 4, 2016, https://iapp.org/news/a/hamburgs-dpa-aiming-to-challenge-privacy-shield/?mkt_tok-=eyJpIjoiTldaaU1XRmpZek01WTJVe-iIsInQiOiJBQ09zSmJUYmxXdUFB-d0FwVElpamswbGZqckVhc0RISUxnRUpaK2FXYU9QcEdvZkpmK2JD-VEp1bHZmQ3FFVDRCYWRK1JR-V1U4ZkR3bGtzbTRXeHhsXC8zY-WQ0VENXdjdhcjV6MVlMXC83eD-JZPSJ9.

79 EuGH: U. v. 08.04.2014. Verb. Rs. C-293/12 und C-594/12. Digital Rights Ireland und Seitlinger u. a. ECLI:EU:C:2014:238.

80 Z.Z. nur auf Englisch verfügbar: Action brought on 16 September 2016 —

Digital Rights Ireland v Commission (Case T-670/16). Official Journal of the European Union. C 410/26, 07.11.2016, S. 26-27.

81 EuGH: Rs. C-362/14 (Schrems), Rn. 66 sowie Tenor, Zi. 1.

82 WP29: Stellungnahme 7/2014 (a. a. O., Fn. 19).

83 Mortsiefer (2011) (a. a. O., Fn. 8), S. 238: ohne AntiDopG „fraglich“, da „keine straf- oder nebenstrafrechtlichen Tatbestände, die einen dringenden Informationsaustausch rechtfertigen könnten“.

84 S. Simitis, in Simitis (2014) (a. a. O., Fn. 50), Einl. Rn. 35.

85 Im Vorschlag der Kommission als Art. 7 Abs. 1 lit. 4 vorgesehen, vom Parlament ausdrücklich unterstützt, im Ergebnis aus dem Art. 7 gestrichen, jedoch als EG 34 beibehalten. Siehe Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung). Brüssel, den 25.01.2012. KOM(2012) 11 endgültig.

86 WP29: Stellungnahme 15/2011 zur Definition von Einwilligung. Angenommen am 13. Juli 2011. WP187. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_de.pdf, S. 8.

87 Simitis, S.: Die informationelle Selbstbestimmung – Grundbedingung einer verfassungskonformen Informationsordnung. NJW, 1984:8, 398-405.

88 BVerfG, U. v. 15.12.1983, Az. 1 BvR 209, 269, 362, 420, 440, 484/83) (Volkszählung).

89 S. Simitis, in Simitis (2014) (a. a. O.), § 4a Rn. 3.

90 WP29: Stellungnahme 15/2011 (a. a. O, Fn. 83), S. 16; wortgleich zitiert aus: WP29: Stellungnahme 8/2001 zur Verarbeitung personenbezogener Daten von Beschäftigten. Angenommen am 13. September 2001. WP 48. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_de.pdf, S. 27.

91 Z. B. S. Simitis, in Simitis (2014) (a. a. O., Fn. 50), § 4a Rn. 62.

92 WP29: Zweite Stellungnahme 4/2009, S. 12.

93 “Each government will put in place legislation, regulation, policies or administrative practices for cooperation and sharing of information with Anti-Doping Organizations and sharing of data among Anti-Doping Organizations as provided in the Code.”

94 S. Simitis, in Simitis (2014) (a. a. O., Fn. 50), § 4c Rn. 19.

95 S. Simitis, in Simitis (2014) (a. a. O., Fn. 50), § 4c Rn. 19.

96 Rechtsgutachten Wedde (a. a. O., Fn. 41), S. 151-152.

97 Zu dem sich die Bundesregierung im Gesetzesentwurf ausdrücklich bekannt hat, siehe BT-Drucksache 18/4898 (a. a. O., Fn. 5).

98 “Rather than look for a single needle in the haystack, [the] approach was, ‘Let’s collect the whole haystack.’ ” Zit. n. Nakashima, E./Warrick, J.: For NSA chief, terrorist threat drives passion to ‘collect it all’. Washington Post, July 14, 2013, https://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html.

99 EuGH: U. v. 08.04.2014. Verb. Rs. C-293/12 und C-594/12. Digital Rights Ireland und Seitlinger u. a. ECLI:EU:C:2014:238 (Digital Rights Ireland), Rn. 65.

100 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15.03.2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG. ABl. EU L 105, 13.04.2006, S. 54–63.

101 Senécal (2009) (a. a. O., Fn. 60), S. 14.

102 WADA: July 26, 2004. WADA signs agreement for development of Clearinghouse computer system. ADAMS System to Facilitate Worldwide Testing Coordination. https://www.wada-ama.org/en/media/news/2004-07/wada-signs-agreement-for-development-of-clearinghouse-computer-system.

103 EuGH: U. v. 18.07.2006. Rs. C-519/04 P. David Meca-Medina und Igor Majcen gegen Kommission der Europäischen Gemeinschaften. Slg. 2006 I-06991. ECLI:EU:C:2006:492, Rn. 40.

104 Siehe Art. 2 (“Guiding principles”) lit. d): “protection of private life and personal data”, Art. 14 (“Personal data protection”) sowie Art. 34 (“Conditions and safeguards”).

105 BT-Drucksache 18/4898 (a. a. O., Fn. 5)

106 BT-Drucksache 18/4898 (a. a. O., Fn. 5), S. 7.

107 BT-Drucksache 18/4898 (a. a. O., Fn. 5), S. 53.

108 BT-Drucksache 18/4898 (a. a. O., Fn. 5), S. 38.

109 BT-Drucksache 18/489 (a. a. O., Fn. 5), S. 38.

110 BT-Drucksache 18/4898 (a. a. O., Fn. 5), S. 38.

111 Stellungnahme der Datenschutzbeauftragten der Länder Rheinland-Pfalz und Schleswig-Holstein zum Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz und des Bundesministeriums des Innern Entwurf eines Gesetzes zur Bekämpfung von Doping im Sport (nicht veröffentlichte Version, Bearbeitungsstand 01.09.2014). https://www.datenschutz.rlp.de/aktuell/2014/images/Anti-Doping-GE_RLP_SH.pdf

112 Stellungnahme LfD RP u. SH (01.09.2014) (a. a. O., Fn. 111), S. 8.

113 Stellungnahme LfD RP u. SH (01.09.2014) (a. a. O., Fn. 111), S. 9.

114 So z. B. Art. 5.8 WADC (a. a. O., Fn. 7): “Anti-Doping Organizations shall ensure they are able to do each of the following, as applicable and in accordance with the International Standard for Testing and Investigations: 5.8.1 Obtain, assess and process anti-doping intelligence from all available sources to inform the development of an effective, intelligent and proportionate test distribution plan, to plan Target Testing, and/or to form the basis of an investigation into a possible anti-doping rule violation(s); and 5.8.2 Investigate Atypical Findings and Adverse Passport Findings, in accordance with Articles 7.4 and 7.5 respectively; and 5.8.3 Investigate any other analytical or non-analytical information or intelligence that indicates a possible anti-doping rule violation(s), in accordance with Articles 7.6 and 7.7, in order either to rule out the possible violation or to develop evidence that would support the initiation of an anti-doping rule violation proceeding.”

115 So z. B. Art. 4.9.3 ISTI (a. a. O., Fn. 9): „Anti-Doping Organizations should consult and coordinate with each other, with WADA, and with law enforcement and other relevant authorities, in obtaining, developing and sharing information and intelligence that can be useful in informing Test Distribution Planning, in accordance with Section 11.0 of the International Standard for Testing and Investigations.”

116 So z. B. Art. 11.2.2 ISTI (a. a. O., Fn. 9): 11.2.2 Anti-Doping Organizations shall

have policies and procedures in place to ensure that anti-doping intelligence captured or received is handled securely and confidentially, that sources of intelligence are protected, that the risk of leaks or inadvertent disclosure is properly addressed, and that intelligence shared with them by law enforcement, other relevant authorities and/or other third parties, is processed, used and disclosed only for legitimate anti-doping purposes." Siehe auch Art. 12.3.1 ISTI: "Anti-Doping Organizations shall ensure that they are able to investigate confidentially and effectively any other analytical or nonanalytical information or intelligence that indicates there is reasonable cause to suspect that an anti-doping rule violation may have been committed, in accordance with Code Articles 7.6 and 7.7, respectively."

117 Lov om fremme af dopingfri idræt, L. 1438 af 22/12/2004, https://www.retsinformation.dk/Forms/r0710.aspx?id=11948

118 Serious Organised Crime and Police Act 2005 (Disclosure of Information by SOCA) Order 2010 (SI 2010/1955), http://www.legislation.gov.uk/uksi/2010/1955/pdfs/uksi_20101955_en.pdf

119 "The functions of United Kingdom Anti-Doping Limited (a company limited by guarantee with registration number 6990867) when it is acting as a national anti-doping organisation are designated for the purposes of section 33 of the Serious Organised Crime and Police Act 2005, being functions which appear to the Secretary of State to be functions of a public nature." (ebda.)

120 Stellungnahme LfD RP u. SH (01.09.2014) (a. a. O., Fn. 111), S. 9.

121 Stellungnahme LfD RP u. SH (01.09.2014) (a. a. O., Fn. 111), S. 9.

122 Stellungnahme LfD RP u. SH (01.09.2014) (a. a. O., Fn. 111), S. 9.

123 Stellungnahme LfD RP u. SH (01.09.2014) (a. a. O., Fn. 111), S. 10.

124 Stellungnahme LfD RP u. SH (01.09.2014) (a. a. O., Fn. 111), S. 12.

125 Stellungnahme LfD RP u. SH (01.09.2014) (a. a. O., Fn. 111), S. 12.

126 WADA: Comments. Agenda Item # 5.1. (undatiert).

127 dpa: WADA befürchtet Schaden durch EU-Datenschutzreform, 21.05.2012, 20:09 Uhr, dpa, http://www.t-online.de/sport/id_56593646/wada-befuerchtet-schaden-durch-eu-datenschutzreform.html.

128 M. Kuschewsky, in Kuschewsky (2014) (a. a. O., Fn. 56), S. 261

129 EOC EU Office: The EOC EU Office discusses the data protection reform with EU institutions. Created on Friday, 17 Apr 2015 00:00:00. http://www.euoffice.eurolympic.org/blog/eoc-eu-office-discusses-data-protection-reform-eu-institutions.

130 EuGH: U. (Große Kammer) v. 09.11.2010. Verb. Rs. C-92/09 und C-93/09. Volker und Markus Schecke GbR (C-92/09) und Hartmut Eifert (C-93/09) gegen Land Hessen. Slg. 2010 I-11063. ECLI:EU:C:2010:662 (Schecke), Rn. 48.

131 EuGH: U. (Große Kammer) v. 29.06.2010. Rs. C-28/08 P. Europäische Kommission gegen The Bavarian Lager Co. Ltd. Slg. 2010 I-06055. ECLI:EU:C:2010:378. EuGH, 29.06.2010 (Bavarian Lager).

132 EuGH: U. (Große Kammer) v. 13.05.2014. Rs. C-131/12. Google Spain SL und Google Inc. gegen Agencia Española de Protección de Datos (AEPD) und Mario Costeja González. ECLI:EU:C:2014:317 (Google Spain).

133 EuGH, 06.10.2015 (Schrems).

134 High Court of England and Wales: Judith Vidall-Hall, Robert Hahn and Marc Bradshaw v Google Inc. [2015] EWCA Civ 311. Judgment of 27 March 2015. Case No: A2/2014/0403. (https://www.judiciary.gov.uk/wp-content/uploads/2015/03/google-v-vidal-hall-judgment.pdf) (Vidall-Hall).

135 WADA: WADC (a. a. O., Fn. 7), S. 11.

136 WP29: Stellungnahme 04/2014 zur Überwachung der elektronischen Kommunikation zu nachrichtendienstlichen und nationalen Sicherheitszwecken. Angenommen am 10. April 2014. WP 215, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_de.pdf, S. 3.

137 WP29: Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees). Adopted on 13 April 2016. WP 237. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf, S. 6.

138 WP29: Working Document 01/2016. WP 237, S. 12.

139 Vgl. dazu Kornbeck, J.: Transferring athletes' personal data from the EU to third countries for anti-doping purposes: applying Recital 112 GDPR in the post-Schrems era. IDPL (erscheint demnächst).

140 Nach eigenen Angaben soll die UEFA international tätige 56 Kontrolleure beschäftigen, so UEFA: Anti-Doping. Last updated: 05/10/15 14.05CET, http://www.uefa.org/protecting-the-game/anti-doping/.

141 Deutscher Bundestag: Wiss. Dienste (2014) (a. a. O., Fn. 17), S. 23.

142 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates. ABl. EU L 119, 04.05.2016, S. 89–131.

143 Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27.04.2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität. ABl. EU L 119, 04.05.2016, S. 132–149.

144 EuGH: 08.042014 (Digital Rights Ireland), Rn. 65.

145 „Die Übermittlung von Daten an staatliche Stellen im Ausland unterliegt den allgemeinen verfassungsrechtlichen Grundsätzen von Zweckänderung und Zweckbindung. Bei der Beurteilung der neuen Verwendung ist die Eigenständigkeit der anderen Rechtsordnung zu achten. Eine Übermittlung von Daten ins Ausland verlangt eine Vergewisserung darüber, dass ein hinreichend rechtsstaatlicher Umgang mit den Daten im Empfängerstaat zu erwarten ist." BVerfG, U. des Ersten Senats vom 20.04.2016 - 1 BvR 966/09 - Rn. (1-29), Leitsätze, Rn. 3.

146 Siehe Leitfaden der SIS II Supervision Coordination Group: A Guide for exercising the right of access. Issued in October 2014 - Updated in October 2015, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Large_IT_systems/SIS/15-10-12_SIS_II_GUIDE_OF_ACCESS_UPDATED_2015_EN.pdf.

147 Bundesministerium des Innern: Bonn, den 10.10.2013. Expertengespräch zur Dopinggesetzgebung am 26. September 2013 im Bundesministerium des Innern, Bonn. Leitthemen/

Fragenkatalog (kursiv) mit zugehörigen Antworten/Beiträgen, (https://www.bmi.bund.de/SharedDocs/Downloads/DE/Kurzmeldungen/bericht.pdf?__blob=publicationFile), S. 28-30, S. 50.

148 Ludwig, K.: ARGE Sportrecht des DAV, Frankfurt a.M., 04./05.092015. CaS, 3/2015:1, 334-335.

149 Lehner, M.: Fehlende Verfassungskonformität des geplanten Anti-Doping-Gesetzes. CaS, 2/2015, 130-135.

150 Schültke, A.: Beschwerde vor dem Bundesverfassungsgericht Ist das Anti-Doping-Gesetz verfassungswidrig? Deutschlandfunk, 20.03.2016, http://www.deutschlandfunk.de/beschwerde-vor-dem-bundesverfassungsgericht-ist-das-anti.1346.de.html?dram:article_id=348923.

151 S. Schenk/S. Brink: Offener Brief an DOSB-Präsidenten. Das Chaos ist komplett. FAZ, 23.02.2015, http://www.faz.net/aktuell/sport/sportpolitik/doping/anti-doping-gesetz-offener-brief-an-dosb-praesident-hoermann-13440380.html?printPagedArticle=true#pageIndex_2.

152 Stellungnahme LfD RP u. SH (01.09.2014) (a. a. O., Fn. 111), S. 15.

153 U. Steiner, Die Bekämpfung von Sportmanipulation mit den Mitteln des Strafrechts aus verfassungsrechtlicher Sicht, in: Württembergischen Fußballverband e. V. (Hrsg.), 40 Jahre wfv-Sportrechtsseminare: 1975-2015 - Nationales und internationales Sportrecht im Überblick, S. 17-30.

154 dpa: De Maizière: Anti-Doping-Gesetz gut für Olympia-Chancen. dpa – Mi., 12.11.2014, https://de.nachrichten.yahoo.com/maizi%C3%A8re-anti-doping-gesetz-gut-f%C3%BCr-olympia-chancen-104816726.html.

155 BGH: 07.062016 - KZR 6/15. Nr. 97/2016 (Pechstein), Rn. 66.

156 BGH: 07.062016 - KZR 6/15. Nr. 97/2016 (Pechstein), Rn. 54.

157 BGH: 07.06.2016 - KZR 6/15. Nr. 97/2016 (Pechstein), Rn. 54.

158 Swire, P.S./Ahmad, K./McQuay, T.: Foundations of Information Privacy and Data Protection: A Survey of Global Concepts, Laws and Practice. Portsmouth, NH 2012: IAPP., S. 34-45.

159 Dazu ganz klassisch, wenn auch nicht unangefochten Whitman, J.Q.: The Two Western Cultures of Privacy: Dignity versus Liberty. YLJ 113 (2004), 1151- 1221.

160 Greenleaf (2012) (a. a. O., Fn. 57).

161 Greenleaf (2012) (a. a. O., Fn. 57), S. 92.

162 Kornbeck, J.: The Stamina of the Bosman Legacy: the European Union and the revision of the World Anti-Doping Code (2011-13). MJECL, 22:2 (2015), 283-304.

163 So Koops, B.J.: The trouble with European data protection law. IDPL, 4:4 (2014), 250- 261; siehe jedoch die Aufsicht der Berliner Datenschutzbehörde 1995 bei Citicorp in New York zum Produkt BahnCard, S. Simitis, in Simitis (2014) (a. a. O., Fn. 50), § 4c Rn. 49.

164 Kuner, Ch.: Extraterritoriality and regulation of international data transfers in EU data protection law. IDPL 5:4 (2015), 235-245.

165 Taylor, M.: The EU's human rights obligations in relation to its data protection laws with extraterritorial effect. IDPL 5:4 (2015), 246-256.

166 Schaar, P.: Globale Überwachung und digitale Souveränität. ZfAS, 8:4 (2015), 447-459.

167 Kornbeck, J.: Private Regulation and Public Trust: why increased transparency could strengthen the fight against doping. DZSM, 66: 5 (2015), 121-127.

168 Moston, S./Engelberg, T./Skinner, J.: Athletes' and coaches' perceptions of deterrents to performance-enhancing drug use. IJSPP 7:4 (2015), 623-636. Siehe auch Efverström, A./Ahmadi, N./Hoff, D./Bäckström, Å.: Anti-doping and legitimacy: an international survey of elite athletes' perceptions. IJSPP, advance access (2016), DOI:10.1080/19406940.2016.1170716.

169 Ryan, K.: Doping and anti-doping: the excesses of enterprise and the tyranny of transparency. ISJPP 7:4 (2015), 637-653.

170 WP29: Arbeitspapier vom 25. November 2005. WP 114. (a. a. O., Fn. 62), S. 237.

171 Figura, L.: Doping: Zwischen Freiheitsrecht und notwendigem Verbot. Aachen 2009: Meyer & Meyer Sport (Sportforum 20).

172 Tokarski, W./Steinbach, D.: Spuren. Sportpolitik und Sportstrukturen in der Europäischen Union. Aachen 2001: Meyer & Meyer.

173 EuGH: 15.12.1995 (Bosman) (a. a. O., Fn. 60).

174 BGH: 07.062016 - KZR 6/15. Nr. 97/2016 (Pechstein), Tenor, Punkt d).

175 Anti-Doping Rules applicable to the XXII Olympic Winter Games in Sochi, in 2014. IOC Anti-Doping Rules 2014 – 29.07.2013 (F), http://www.olympic.org/Documents/Games_Sochi_2014/Anti-doping/IOC_Anti-Doping_Rules_Sochi_2014-eng.pdf, Articles 3.2.4, 4.5.1.2, 5.13.

176 11 October 2013. E-011650-13. Question for written answer to the Commission. Rule 117. Christine De Veyrac (PPE). Subject: Surveillance of communications at the Winter Olympic Games in Sochi. http://www.europarl.europa.eu/sides/getDoc.do?type=WQ&reference=E-2013-011650&language=NL.

177 WADA: Minutes of the WADA Foundation Board Meeting. 18 November 2012, https://www.wada-ama.org/sites/default/files/resources/files/wada_fb_18_nov_2012_eng_final.pdf, S. 17.

178 Anti-Doping Reform: Did Anti Doping officials knowingly circumvent EU data protection standards in Sochi? February 22, 2014, https://antidopingreform.wordpress.com/2014/02/22/did-anti-doping-officials-knowingly-circumvent-eu-data-protection-standards-in-sochi/.

179 Zur Unterscheidung siehe Docksey, Ch.: Articles 7 and 8 of the EU Charter: two distinct fundamental rights. In: Grosjean, J. (Hrsg.): Les enjeux européens et mondiaux de la protection des données personnelles. Brüssel 2014: Larcier, 63-89. Ferner Docksey, Ch.: Four fundamental rights: finding the balance. IDPL, 6:3 (2016), 195-209.

Stellungnahme der Deutschen Vereinigung für Datenschutz e. V. (DVD)

Referentenentwurf des Bundesministeriums der Justiz und des Innern

Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU) – Kabinettsvorlage für den 01.02.2017

A Allgemeine Erwägung

Es wird begrüßt, dass der Bundesgesetzgeber ein Gesetz zur Umsetzung der Europäischen Datenschutzgrundverordnung (EU 2016/679, künftig DSGVO) sowie der der Europäischen Datenschutzrichtlinie für Justiz und Inneres (EU 2016/680, künftig JI-Richtlinie) anstrebt. Die Anwendenden der Regelungen benötigen einen rechtssicheren Überblick darüber, welche europäischen und nationalen Regelungen Gültigkeit haben, wenn die DSGVO und die JI-Richtlinie im Mai 2018 direkte Wirksamkeit entfalten.

B Einzelstellungnahme zum Entwurf eines neuen BDSG

Zu § 1 Anwendungsbereich des Gesetzes

Die Regelung in Abs. 2 S. 3, wonach „die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen“, unberührt bleibt, ist unklar. Es trifft zwar zu, wie in der Begründung ausgeführt, dass die Regelung dem bisherigen § 1 Abs. 3 S. 2 BDSG entspricht. Die bisherige Regelung war aber auch schon bisher nicht in der Lage, das komplizierte Verhältnis zwischen besonderen Geheimnissen und Datenschutzrecht zu klären. Durch die Formulierung „die nicht auf gesetzlichen Vorschriften beruhen“ wird der falsche Eindruck vermittelt, dass untergesetzlich Berufsgeheimnisse normiert werden könnten, was unter dem Regime der DSGVO nicht zutreffen kann. Ob implizit ein Verweis auf Berufsordnungen von Heilberufskammern gemeint ist, bleibt unklar. Auf den Halbsatz kann und sollte deshalb verzichtet werden.

Zu § 2 Begriffsbestimmungen

Es wird darauf hingewiesen, dass durch das Außerkrafttreten des **bisherigen Bundesdatenschutzgesetzes** (BDSG-alt) gemäß Art. 8 am 25.05.2018 auch die darin enthaltenen Begriffsbestimmungen aufgehoben werden, auf die weiterhin in Kraft befindliche spezifische Regelungen im deutschen Recht Bezug nehmen. Es wird deshalb angeregt, insofern eine Übergangsregelung vorzusehen.

Zu § 3 Verarbeitung durch öffentliche Stellen

Die Regelung ist wegen Art. 6 Abs. 1 lit. e und außerhalb des Anwendungsbereichs der Verordnung 2016/679 wegen bereichsspezifischen Regelungen überflüssig, aber auch unschädlich. Es wird empfohlen, eine explizite Bezugnahme zu Art. 6 Abs. 1 lit. e DSGVO aufzunehmen.

Zu § 4 Videoüberwachung

Eine **materielle Sonderregelung** zur Videoüberwachung ist unzulässig, da insofern Art. 6 DSGVO weitgehend abschließend ist (Kühling/Martini u. a. S. 343 ff.; Roßnagel, Europäische Datenschutz-Grundverordnung, 2016, S. 52 f.).

Dies gilt auch für den geplanten Abs. 1 S. 2, wonach bei Videoüberwachung in **„öffentlich zugänglichen öffentlichen Anlagen** … oder Fahrzeugen und öffentlich zugänglichen großflächigen Einrichtungen des Schienen-, Schiffs- und Bahnverkehrs … der Schutz von Leben, Gesundheit oder Freiheit der dort aufhältigen Personen als besonders wichtiges Interesse“ gilt. Diese Regelung gibt zwar inhaltlich eine Selbstverständlichkeit wider. Zweck und voraussichtliche Wirkung dieser Regelung ist aber, dass im Rahmen der Interessenabwägung bei öffentlicher Videoüberwachung den Sicherheitsinteressen der Vorrang eingeräumt wird.

Zudem nimmt die auch für private Stellen geltende Regelung diese für öffentliche **polizeiliche Sicherheitsbelange** in Anspruch und verletzt dadurch die Gesetzgebungsbefugnis der Länder, den Verhältnismäßigkeitsgrundsatz sowie spezifische Grundrechte wie z. B. das Versammlungsrecht gemäß Art. 8 GG. Viele Länder haben von ihrer Befugnis Gebrauch gemacht, Videoüberwachung in ihrem Versammlungsrecht zu regulieren. Der vorliegende Entwurf steht hierzu sowohl formal wie auch inhaltlich im Widerspruch.

Dieses Ergebnis wird verstärkt durch die Regelung in Abs. 3, die bei Erforderlichkeit „zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten“ **ohne eine Angemessenheitsprüfung** eine Zweckänderung erlaubt. Auf die gesonderte Stellungnahme der DVD und des Netzwerks Datenschutzexpertise vom 06.11.2016 wird verwiesen (https://www.datenschutzverein.de/wp-content/uploads/2016/11/Stellungnahme_Videoueberwachung_06112016.pdf).

Gemäß Abs. 2 ist der Umstand und der Verantwortliche der Videoüberwachung **„zum frühestmöglichen Zeitpunkt er-**

kennbar zu machen“. Die zeitliche Bezugnahme macht keinen Sinn und verursacht in der praktischen Umsetzung Probleme: Findet im öffentlichen Raum eine Videoüberwachung statt, so kann und muss diese sofort kenntlich gemacht werden.

Die Erkennbarkeit von Videoüberwachung ist wegen der teilweise bestehenden räumlichen Verhältnisse oft schwer zu realisieren. Als zusätzliche Gewährleistungsmaßnahme für Transparenz sollte daher eine **Meldepflicht** sämtlicher öffentlicher Videokameras vorgesehen werden, kombiniert mit einer Veröffentlichung im Internet. Dies hätte nicht nur einen Transparenzgewinn für die Betroffenen, sondern auch für Sicherheitsbehörden zur Folge, die so im Bedarfsfall sofort feststellen können, wo im Fall einer Ermittlungsnotwendigkeit evtl. Bildmaterial erstellt worden ist.

Bei Videoüberwachung im öffentlichen Raum sollte zudem eine Pflicht zur **Datenschutz-Folgenabschätzung** nach Art. 35 DSGVO normiert werden, die dazu führt, dass durch Marktnachfrage Hersteller datenschutzfreundlich gestaltete, dokumentierte oder gar zertifizierte Produkte anbieten (s. u. D).

Zu § 8 Errichtung Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)

In Abs. 1 S. 2 ist vorgesehen, dass der Sitz der BfDI **Bonn** sein soll. Angesichts der hohen grundrechtspolitischen Bedeutung der Stelle der BfDI ist es nicht sinnvoll, diese weiterhin derart weit von den politisch relevanten Gremien in Berlin zu lokalisieren. Daher sollte als Sitz Berlin festgelegt werden oder zumindest auf eine gesetzliche Festlegung vollständig verzichtet werden.

Zu § 11 Ernennung und Amtszeit der BfDI

Die § 22 Abs. 1 **BDSG-alt übernehmende** Regelung des Abs. 1 sieht vor, dass der deutsche Bundestag die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) „ohne Aussprache auf Vorschlag der Bundesregierung (…) mit mehr als der Hälfte der gesetzlichen Zahl seiner Mitglieder“ wählt. Die Wahl setzt voraus, dass die BfDI „das 35. Lebensjahr vollendet“ hat. In Abs. 1 S. 4 wird geregelt: „Sie oder er muss über die für die Erfüllung ihrer oder seiner Aufgaben und Ausübung ihrer oder seiner Befugnisse erforderliche Qualifikation, Erfahrung und Sachkunde insbesondere im Bereich des Schutzes personenbezogener Daten verfügen. Insbesondere muss die oder der Bundesbeauftragte über durch einschlägige Berufserfahrung nachgewiesene Kenntnisse des deutschen und europäischen Datenschutzrechts verfügen und die Befähigung zum Richteramt oder höheren Dienst haben.“ Gemäß Abs. 3 ist bei einer Amtszeit von 5 Jahren eine einmalige Wiederwahl zulässig.

Die Beachtung rechtlicher Anforderungen an das Bestellungsverfahren und an die Qualifikation der Datenschutzbeauftragten stand lange Zeit nicht im Fokus öffentlicher Diskussion. Dies hat sich mit dem Gutachten des **Netzwerks Datenschutzexpertise** vom 17.11.2016 geändert, in dem sowohl die rechtlichen Anforderungen wie auch die Praxis kritisch hinterfragt werden. Dabei erweist sich, dass die bisherige Praxis, die mit dem vorliegenden Regelungsvorschlag fortgeschrieben werden soll, gegen Vorgaben des Europarechts und des Verfassungsrechts verstößt (http://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2016_auswahlblfdi6.pdf).

Der Regelungsvorschlag sieht keine öffentliche Ausschreibung der Stelle der BfDI vor und schließt ausdrücklich eine Aussprache über die Wahl aus. Dies steht in Widerspruch zu Art. 53 Abs. 1 DSGVO, wonach das Mitglied der Aufsichtsbehörde „im Wege eines **transparenten Verfahrens** ernannt wird“. Die Transparenzanforderung zielt auf eine öffentliche demokratische Debatte zur Bestellung und die Gewährleistung einer hohen Legitimation und gleicher Chancen der qualifizierten Kandidaten ab. Dies war bisher und würde auch künftig nicht gewährleistet. Die geplante Regelung ist insofern europarechtswidrig.

Art. 33 Abs. 2 Grundgesetz (GG) ist zu beachten, wonach jeder Deutsche „nach seiner Eignung, Befähigung und fachlichen Leistung gleichen Zugang zu jedem öffentlichen Amt“ hat.

Das Erfordernis eines **Mindestalters** von 35 Jahren stellt eine nicht gerechtfertigte Altersdiskriminierung dar (Art. 3 Abs. 1 GG, Art. 21 Abs. 1 Europäische Grundrechte-Charta – GRCh). Die abschließenden persönlichen Anforderungen des Art. 53 Abs. 2 DSGVO stellen nicht auf das Alter ab. Der Verweis der Gesetzesbegründung (S. 77) auf Art. 54 Abs. 1 lit. b DSGVO („sonstige Voraussetzungen“) legitimiert keine unsachlichen Anforderungen. Personen unter 35 Jahren können die geforderte Erfahrung und Sachkunde vorweisen. Diese Regelung ist daher verfassungs- und europarechtswidrig.

Das Erfordernis der Befähigung zum **Richteramt oder höheren Dienst** war historisch begründet, als die Datenschutzbeauftragten weitgehend nur für die Kontrolle des öffentlichen Bereichs zuständig waren. Das Erfordernis findet sich nicht in Art. 53 Abs. 2 DSGVO und ist auch keine adäquate Beschreibung der Qualifikation und Sachkunde. Daher sollte auf diese Einschränkung verzichtet werden.

Die Beschränkung auf eine **einmalige Wiederwahl** findet sich nicht in der abschließenden Aufzählung der personellen Anforderungen an das Mitglied der Aufsichtsbehörde in Art. 53 Abs. 2 DSGVO. Amtsinhaber, die zwei Amtsperioden absolviert haben, können regelmäßig die dort geforderte Erfahrung, Qualifikation und Sachkunde vorweisen. In der Praxis hat sich gezeigt, dass durch mehrfach wiedergewählte Datenschutzbeauftragte eine qualifizierte Amtsausübung gewährleistet wird. Angebliche Gründe für eine Beschränkung, etwa Erlahmen der Innovationsbereitschaft, treffen nicht zu. Es gibt keine Wiederwahlverbote in vergleichbaren Positionen. Diese Regelung ist daher verfassungs- und europarechtswidrig.

Zu § 13 Rechte und Pflichten der BfDI

In Abs. 5 S. 2 ist vorgesehen, dass die BfDI keine **Aussagebefugnis als Zeugin** hat, soweit die Aussage laufende oder abgeschlossene Vorgänge betrifft, „die dem Kernbereich exekutiver Eigenverantwortung der Bundesregierung zuzurechnen sind oder sein könnten“. In diesen Fällen muss das „Benehmen mit der Bundesregierung“ hergestellt werden. Was zum Kernbe-

reich exekutiver Eigenverantwortung der Bundesregierung zu zählen ist, ist völlig unklar. Dadurch, dass schon die theoretische Möglichkeit eines solchen Betroffenseins dazu führt, dass die Aussagebefugnis von einem Benehmen mit der Bundesregierung abhängig gemacht wird, wird die Unabhängigkeit der BfDI unangemessen beeinträchtigt. Es wird vorgeschlagen, insofern eine Kann-Regelung bzgl. der Aussageverweigerung vorzusehen sowie eine Sollregelung in Bezug auf das Benehmen mit der Bundesregierung.

Zu § 14 Aufgaben der BfDI

Die DSGVO sieht als Aufgabe von Aufsichtsbehörden auch „Datenschutzzertifizierungsmechanismen und von **Datenschutzsiegeln und -prüfzeichen** nach Artikel 42 Absatz 1“ vor. (Art. 57 Abs. 1 lit. n DSGVO). Datenschutz-Zertifizierung gibt es bisher in Deutschland nur auf Länderebene und ist auch künftig als Aufgabe für die BfDI nicht vorgesehen. Dies entspricht nicht den aktuellen technischen und rechtlichen Erfordernissen, die in der DSGVO erkannt und festgelegt werden.

Zu § 16 Befugnisse der BfDI

In Abs. 2 ist vorgesehen, dass außerhalb des Anwendungsbereichs der DSGVO bei der Feststellung von Datenschutzverstößen durch öffentliche Stellen – wie bisher – lediglich als „Sanktion“ eine Beanstandung zulässig ist. Diese Regelung ignoriert die Regelungsintention des neuen europäischen Datenschutzrechts, angesichts der großen Umsetzungsdefizite beim Datenschutz – auch im öffentlichen Bereich – wirksame Sanktionen zu ermöglichen. **Beanstandungen** haben sich insbesondere im Sicherheitsbereich oft als wirkungslos erwiesen, da sie kein rechtliches Instrument sind, mit dem Verantwortliche zu rechtskonformem Vorgehen gebracht werden können. Dies haben u. a. die Datenschutzverstöße durch den Bundesnachrichtendienst (BND) gezeigt, die nach den Offenlegungen von Edward Snowden bekannt geworden sind. Mit der Regelung wird gerade im Bereich der JI-Richtlinie sowie der Geheimdienste auf eine effektive Sanktionsform verzichtet. Sollen finanzielle Sanktionen sowie Unterlassungs- und Beseitigungsverfügungen nicht möglich sein, so muss der BfDI zumindest ein Klagerecht vor Gericht gegen rechtswidrige Datenverarbeitung eröffnet werden.

Die Regelung des Abs. 3 S. 1, wonach sich die Befugnisse der BfDI auch auf **Post- und Telekommunikationsgeheimnisse sowie auf Steuergeheimnisse** erstrecken, ist historisch begründet und inzwischen eine Selbstverständlichkeit, welcher es nicht bedarf. Auf sie sollte deshalb verzichtet werden.

Zu § 17 Vertretung im Europäischen Datenschutzausschuss (EDSA)

In Abs. 1 ist vorgesehen, dass die BfDI die gemeinsame Vertretung Deutschlands im Datenschutzausschuss (EDSA) wahrnimmt. Die Stellvertretung soll aus den Leitungen der Landes-Aufsichtsbehörden vom Bundesrat ausgewählt werden. Bei Angelegenheiten, die insbesondere die Länderaufsicht betreffen, soll nach Abs. 2 im EDSA vorrangig die Stellvertretung tätig werden. Diese Regelung ist nicht sachgerecht und beeinträchtigt die Unabhängigkeit der Landesaufsichtsbehörden.

Hauptaufgabe des EDSA wird die Festlegung von Positionen im Bereich des **Datenschutzes im nicht-öffentlichen Bereich** (oder in der Begrifflichkeit der DSGVO: **für Unternehmen**) sein. Insofern hat die BfDI – abgesehen von Post- und Telekommunikationsunternehmen – weder Kompetenzen noch Erfahrungen. Diese liegen vielmehr bei den Landesaufsichtsbehörden.

Durch die **Bestimmung der Stellvertretung** durch den Bundesrat wird dem Bundesrat die Möglichkeit eröffnet, am Willen der Aufsichtsbehörden vorbei unter Anlegung sachfremder Erwägungen für diese deren Vertretung zu benennen. Dies kann zur Folge haben, dass die dadurch in den EDSA eingebrachten Positionen nicht die der unabhängigen Aufsichtsbehörden repräsentieren. Die Regelung ist völlig unangemessen.

Es wird vorgeschlagen, die Bestimmung der Vertretung und der Stellvertretung der deutschen Aufsichtsbehörden diesen selbst zu überlassen. Diese sollten mit qualifizierter Mehrheit ihre **Vertretung im EDSA selbst wählen**. Dieser Vorschlag entspricht der „Kühlungsborner Erklärung“ der unabhängigen Datenschutzbehörden der Länder vom 10.11.2016 (https://www.datenschutz.de/kuehlungsborner-erklaerung-der-unabhaengigen-datenschutzbehoerden-der-laender-vom-10-november-2016/).

Zu § 18 Verfahren der Zusammenarbeit der Aufsichtsbehörden

Zur Bestimmung von gemeinsamen Positionen der deutschen Aufsichtsbehörden soll gemäß Abs. 2 zunächst ein **Einigungsverfahren** angestrebt werden. Gelingt eine Einigung nicht, so soll der Vertreter bzw. in Länderangelegenheiten der Stellvertreter ein Bestimmungsrecht haben, „wenn nicht die Aufsichtsbehörden von Bund und Ländern einen anderen Standpunkt mit einfacher Mehrheit beschließen“. Wegen der nicht repräsentativen Festlegung der Vertretung (s. o. zu § 17) wird damit in die Unabhängigkeit der Aufsichtsbehörden unangemessen eingegriffen.

Nach Abs. 3 S. 2 soll im Falle, dass eine Einigung unter den deutschen Aufsichtsbehörden nicht möglich ist, der Stellvertreter ein Bestimmungsrecht haben, wenn „die Angelegenheit die Wahrnehmung von Aufgaben betreffen, für welche die Länder alleine das **Recht zur Gesetzgebung** haben, oder welche die Einrichtung oder das Verfahren von Landesbehörden betrifft“. Die Regelung ist unklar: Das Recht der Gesetzgebung liegt in vielen Fällen des Datenschutzrechtes, insbesondere auch im nicht-öffentlichen Bereich, beim Bund, während die hier in Frage stehende Verwaltungskompetenz bei den Ländern liegt. In der Regelung kann auf den Verweis auf die Gesetzgebungskompetenz verzichtet werden.

Zu § 22 Verarbeitung besonderer Kategorien personenbezogener Daten

In der Regelung werden wesentliche Inhalte des Art. 9 DSGVO wiederholt, ohne weitere Präzisierungen vorzunehmen. Diese Regelung ist wegen der reinen **Paraphrasierung** ohne eine zusätzliche Regelungsabsicht rechtswidrig (Kühling/Martini u. a., S. 6 ff. m. w. N.). Auf sie sollte verzichtet werden.

In Abs. 2 werden Aussagen gemacht, was „**angemessene und spezifische Maßnahmen** zur Wahrung der Grundrechte und Interessen der betroffenen Personen“ gemäß Art. 9 Abs. 1 DSGVO sind. Problematisch ist hierbei, dass auf die „Implementierungskosten“ Bezug genommen wird, die in Art. 32 DSGVO bzgl. der informationstechnischen Sicherheit, nicht aber bzgl. der Gestaltung von Verfahren nach Art. 25 DSGVO oder materiell-prozessualen Vorkehrungen relevant sein sollen. Selbstverständlich können solche Kosten bei Angemessenheitsentscheidungen eine Rolle spielen. Deren explizite Erwähnung eröffnet aber die Möglichkeit, spezifische Maßnahmen allein aus Kostengründen zurückzuweisen. Wenig förderlich ist auch der Verweis auf Sensibilisierungs- und Schulungsmaßnahmen (Abs. 2 Satz 2 Nr. 2). Die in Abs. 2 enthaltenen Erwähnungen sind nicht vollständig und weisen erst recht nicht auf eine Priorisierung hin. Die Regelung ist daher nicht geeignet, eine Konkretisierung der europäischen Vorgaben zu bewirken. Daher sollte auf sie verzichtet werden.

Es ist nicht erkennbar, weshalb die Anwendung von Abs. 2 gemäß Satz 3 im Fall des Abs. 1 lit. b (**Datenverarbeitung im Gesundheits- und Sozialbereich durch Berufsgeheimnisträger**) ausgeschlossen wird. Zwar werden auch in Art. 9 Abs. 3 DSGVO mit der Regelung zu Berufsgeheimnisträgern die angemessenen spezifischen Sicherungsmaßnahmen erwähnt, doch erfolgt dies systematisch an einem anderen Ort. Es dürfte nicht bestritten werden können, dass solche Maßnahmen auch und gerade erforderlich sind, wenn hochsensible Daten, die Berufsgeheimnissen unterliegen, verarbeitet werden.

Zu § 23 Zweckänderungen öffentlicher Stellen

In der Norm werden eine Vielzahl von Zweckänderungen erlaubt, die schon derzeit ihre Erlaubnisgrundlage in der DSGVO finden. Insofern sind sie überflüssig und wegen der **reinen Wiederholung** europäischer Normvorgaben unzulässig. In Abs. 1 wurde gegenüber den Vorentwürfen die Sicherung des Steuer- und Zollaufkommens als Rechtfertigung für eine Zweckänderung neu aufgenommen.

Diese Regelungen beziehen sich auf die in Art. 6 Abs. 1 lit. e DSGVO vorgegebenen Verarbeitungsbefugnissen, ohne jedoch bei sämtlichen Alternativen eine **Abwägung mit dem Betroffeneninteressen** vorzusehen. Damit laden diese Regelungen zu einer pauschalen Missachtung dieser Interessen ein und begründen unverhältnismäßige Informationseingriffe durch Zweckänderungen.

Zu § 26 Verarbeitung von Beschäftigtendaten

Die Wiederauflage des **missglückten § 32 BDSG**-alt ist abzulehnen. Diese Norm führte zu Rechtsunsicherheit, nicht zur Präzisierung von Verarbeitungsbefugnissen und Betroffenenrechten. Zudem darf bezweifelt werden, dass die vorgesehene Regelung den Anforderungen des Art. 88 Abs. 2 DSGVO standhält. Es bedarf vielmehr eines umfassenden Beschäftigtendatenschutzgesetzes, wozu das Netzwerk Datenschutzexpertise die relevanten Rahmenbedingungen in seinem Gutachten vom 08.04.2016 benannt hat (http://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2016_dsgvo_beschds.pdf).

Zu § 27 Zwecke der wissenschaftlichen Forschung

Die geplante Forschungsregelung ist unvollständig und unterschreitet das in der DSGVO vorgeschriebene Niveau. Unvollständig ist Abs. 1 im Hinblick auf sensitive Daten gemäß Art. 9 Abs. 1 DSGVO dadurch, dass eine Konkretisierung von angemessenen Schutzmaßnahmen, wie in Art. 9 Abs. 2 lit. j DSGVO gefordert, unterlassen wird. Art. 89 Abs. 1 DSGVO sieht vor, dass die Datenverarbeitung zu „Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken (…) geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person“ zu unterliegen hat. Derartige Schranken enthält der vorgelegte Entwurf nicht. Unvollständig ist die Regelung auch im Hinblick auf die Verarbeitung von Berufsgeheimnissen, z. B. dem Patientengeheimnis unterliegenden Daten, da insofern weiterhin § 203 StGB als Hindernis zur Einbeziehung in Forschungsvorhaben bestehen bleibt. Tatsächlich werden keine ausreichenden und effektiven Schutzmaßnahmen geregelt, sondern lediglich ein Minimalkatalog beliebiger Vorkehrungen. So wird es z. B. unterlassen, ein explizites beschlagnahmesicheres Forschungsgeheimnis festzuschreiben. Unbefriedigend ist die Regelung insgesamt, da sie nicht das Ziel verfolgt, den Wirrwarr unterschiedlicher spezifischer Forschungsklauseln im Bundes- und im Landesrecht zu vereinheitlichen und zu modernisieren. Zur Sicherung des Datenschutzes in der Forschung und einer damit verbundenen Stärkung des Forschungsstandortes Deutschland bedarf es eines umfassenden **Forschungsgesetzes**, das, um auch die Regelungsebene der Länder mit einzuschließen, als Bund-Länder-Staatsvertrag erlassen werden sollte.

Der **Ausschluss des Auskunftsanspruchs** bei Erforderlichkeit für die wissenschaftliche Forschung und einem „unverhältnismäßigen Aufwand“ nach Abs. 2 ist zu unbestimmt und ermöglicht Forschenden mit Pauschalbegründungen die Verweigerung von Transparenz gegenüber den Betroffenen.

Zu § 29 Geheimnisschutz

Die Regelung beschreibt nur völlig unzureichend, welche Daten mit ihr erfasst werden sollen: Die Kennzeichnung von Daten danach, dass diese „nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen des überwiegenden rechtlichen Interesses eines Dritten, geheim gehalten werden müssen“, ist **zu unbestimmt** und kann auf jede Form eines spezifischen Geheimnisses angewendet werden, nicht nur auf Berufsgeheimnisse nach § 203 Abs. 1, (2a,) 3 StGB, § 53, 54 StPO, sondern auch auf das Sozialgeheimnis nach § 35 SGB I, ja sogar auf weitgehend unreguliert bleibende Betriebs- und Geschäftsgeheimnisse. In der Literatur wird diese Regelung – fälschlich – gar auf Amtsgeheimnisse wie z. B. das Statistik- oder das Meldegeheimnis erstreckt (Paal/Pauly, Datenschutz-Grundverordnung, 2016, Art. 90 Rn. 6). Es bedarf vielmehr einer rechtssicheren Verweisung auf einen engen Kranz aus besonderen Gründen gesondert zu behandelnder Daten.

Gemäß dem Absatz 1 werden das Informationsrecht nach Art. 14 DSGVO und das **Auskunftsrecht** nach Art. 15 DSGVO eingeschränkt, wenn die Daten „ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen“. Diese Formulierung ist für alle Beteiligten nicht kalkulierbar und zu unbestimmt. Die Unbestimmtheit der erfassten Daten erstreckt sich auf diese Beschränkung informationeller Selbstbestimmung generell und des Auskunftsanspruchs als „Magna Charta des Datenschutzes“ (s. u. zu § 34). Damit wird die grundlegende Garantie des Auskunftsanspruchs in Art. 8 Abs. 2 S. 2 GRCh verletzt, der Folgendes vorsieht: „Jeder Mensch hat das Recht, Auskunft über die ihn betreffenden erhobenen Daten zu erhalten“. Diese Unbestimmtheit beruht auch auf der völlig offenen Abwägungsnorm, die weder für Anwender noch für Betroffene einschätz- und berechenbar ist. Die Einschränkung des Auskunftsanspruchs muss sich auf spezifische Fallgestaltungen beschränken, die notwendig und verhältnismäßig sind. Die vorliegende Regelung genügt diesen Anforderungen nicht und ist europarechts- und verfassungswidrig.

Auch die Ausnahme von der Informationspflicht in Abs. 2 ist sowohl hinsichtlich des Anwendungsbereichs wie auch des Inhaltes unbestimmt. In der Begründung (S. 105 f.) wird auf die **Kommunikation zwischen Mandanten** von Wirtschaftsprüfern und Rechtsanwälten Bezug genommen, während in der Regelung generell der erheblich weitere Begriff der Berufsgeheimnisträger verwendet wird. Das Kundenverhältnis anderer Berufsgeheimnisträger kann auch als Mandat gekennzeichnet werden. Zudem verwendet die Ausnahmeregelung wieder eine offene, beliebig verwendbare Abwägungsformel.

In Abs. 3 wird bei den in § 203 Abs. 1, 2a und 3 StGB beschriebenen Daten die **Datenschutzkontrolle** durch die zuständige Aufsicht mit unbestimmten Formulierungen unverhältnismäßig beschnitten. Es soll keine Untersuchungsbefugnisse geben, „soweit die Inanspruchnahme der Befugnisse zu einem Verstoß gegen die Geheimhaltungspflichten dieser Personen führen würde“. Bisher ist unbestritten, dass zu den in die Kontrolle einbezogenen Daten auch Berufsgeheimnisse gehören. Bisher gehört die Kontrolle der Wahrung des Patienten- und den Sozialgeheimnisses sogar zu den Schwerpunkten der aufsichtsbehördlichen Tätigkeit. Diese würde massiv behindert, da jeder Verantwortliche sich einer Kontrolle zunächst dadurch entziehen könnte, dass er geltend macht, seine Geheimhaltungspflichten würden verletzt. Im ärztlichen und psychologischen Bereich wurde die Datenschutzkontrolle bisher auch von den geprüften Stellen nicht in Frage gestellt. Sie ist vielmehr oft ein Instrument, um das Vertrauen in die jeweiligen Stellen zu erhöhen.

Der Gesetzentwurf geht von der falschen Annahme aus, dass Datenschutzkontrollen den Datenschutz verletzen könnten. Tatsächlich unterliegen die bei einer Kontrolle erlangten Daten einer strengen Zweckbindung. Es ist in der über 40-jährigen Geschichte der Datenschutzaufsicht noch kein Fall bekannt geworden, dass über Datenschutzkontrollen **Berufsgeheimnisse** offenbart worden wären. Dem kann durch die vorgesehene Regelung, auf die Datenschutzaufsicht die Geheimhaltungspflicht des Verantwortlichen auszuweiten, auch künftig vorgebeugt werden.

Durch die vorgesehene weitgehende Ausnahme von der Datenschutzkontrolle wird das von der DSGVO verfolgte Ziel einer weitgehenden **Harmonisierung** verfehlt. Sie hat auch zur Folge, dass vom Europäischen Datenschutzausschuss gemäß Art. 70 DSGVO erarbeitete Leitlinien, Empfehlungen und bewährte Verfahren nur begrenzt ein- und umgesetzt werden können.

Die Begründung (S. 106) verweist auf die bundesverfassungsgerichtliche Rechtsprechung, wonach das Mandatsverhältnis nicht mit Unsicherheiten hinsichtlich seiner Vertraulichkeit belastet werden darf (BVerfG U. v. 12.04.2005, NJW 2005, S. 1917). Dies schließt eine externe Kontrolle der Rechtmäßigkeit des Berufsgeheimnisträgers nicht aus. Es genügt, dass Abs. 2 S. 2 die Geheimhaltungspflicht auf die Aufsichtsbehörde verlängert und ein Beweisverwertungsverbot im Strafverfahren schafft.

Politisch angegriffen wurde die Kontrollbefugnis der Datenschutzaufsicht im nicht-öffentlichen Bereich bisher ausschließlich durch Anwaltsorganisationen. Praktische Probleme sind in diesem Bereich aber in der 40-jährigen Aufsichtsgeschichte nur in wenigen Einzelfällen aufgetreten, die durch eine Berücksichtigung des **Mandantengeheimnisses** bei der Datenschutzkontrolle aufgelöst werden konnten. Der Anwaltschaft geht es darum, sich der unabhängigen Datenschutzkontrolle nicht zum Schutz der Mandanten und des Mandantengeheimnisses zu entziehen, sondern zur Freistellung von Kontrolle generell. Es ist unbestreitbar, dass auch Anwälte dem Datenschutzrecht unterliegen und unterliegen müssen (ausführlich dazu Weichert NJW 2009, 550 ff.; Weichert in Däubler/Klebe/Wedde/Weichert, Bundesdatenschutzgesetz, 5. Aufl. 2016, § 38 Rn. 11 m. w. N.).

Art. 90 DSGVO erlaubt nur Einschränkungen der Datenschutzkontrolle, die **„notwendig und verhältnismäßig“** sind. Hierzu gibt es weder im Gesetzestext noch in der Begründung Ausführungen. Die geplante Einschränkung ist sachlich nicht zu begründen. Datenschutzverstöße durch Berufsgeheimnisträger werden dadurch vollständig kontroll- und damit auch sanktionsfrei gestellt, so dass die Schutzfunktion unabhängiger Datenschutzkontrolle, die in Art. 8 Abs. 3 GRCh ausdrücklich festgeschrieben ist, verloren geht. Die Regelung ist daher verfassungs- und europarechtswidrig. Auf sie kann und sollte ersatzlos verzichtet werden.

Der Begründung ist auf S. 106 zu entnehmen, dass S. 2 von Abs. 3 sich auf Daten bei **Auftragsverarbeitern von Berufsgeheimnisträgern** beziehen soll. Diese Zielsetzung ist der geplanten Gesetzesformulierung nicht zu entnehmen. Die Begründung verdreht die Rechtslage: Auftragsverarbeiter können im Rahmen einer Datenschutzkontrolle gegenüber ihren Auftraggebern nicht vertragsbrüchig werden. Das rechtliche Problem ist derzeit, dass das Outsourcing personenbezogener Datenverarbeitung seit Jahren einen Verstoß gegen die berufliche Geheimhaltungspflicht darstellt. Es ist zu begrüßen, dass insofern nun vonseiten des Bundesjustizministerium ein Referentenentwurf erarbeitet wurde, der diese rechtlich nicht akzeptable Situation auflöst. Dieser zu begrüßende Entwurf sollte umgehend einge-

bracht und spätestens zeitgleich mit den Umsetzungsregelungen zur DSGVO in Kraft gesetzt werden (s. u. D).

Zu § 31 Schutz des Wirtschaftsverkehrs bei Scoring und Bonitätsauskünften

Die Übernahme dieser Regelungen aus dem BDSG-alt (§§ 28b, 28b) ist in Bezug auf den Regelungsinhalt grundsätzlich zu begrüßen. Es ist aber in Frage zu stellen, ob „die Verwendung eines Wahrscheinlichkeitswerts“, insbesondere im Hinblick auf „die Zahlungsfähig- und Zahlungswilligkeit“ ein „wichtiges Ziel des allgemeinen öffentlichen Interesses“ der Bundesrepublik Deutschland darstellt und damit, ob die Öffnungsklausel aus Art. 6 Abs. 4 i. V. m. Art. 23 Abs. 1 DSGVO greift, so wie dies in der Begründung eines Vorentwurfs zum Kabinettsentwurf erwähnt wurde. Der aktuelle Entwurf äußert sich zur Regelungsberechtigung nicht.

Mit Abs. 1 soll der bisherige § 28b BDSG-alt zum Scoring fortgelten. Es ist fraglich, inwieweit dies durch die abschließenden Regelungen des Art. 6 Abs. 1 DSGVO ausgeschlossen ist. Wenn dies verneint wird, sind gemäß Art. 22 Abs. 2 lit. b DSGVO in jedem Fall angemessene **Maßnahmen zur Wahrung der Rechte und Freiheiten** und berechtigten Interessen der Betroffenen zu gewährleisten (Roßnagel, S. 141; Kühling/Martini u. a., S. 440 ff.). Angesichts der in Deutschland gesammelten Erkenntnisse zum Scoring ist offensichtlich, dass dies nicht der Fall ist. So zeigt sich, dass bei der Eingrenzung der zulässigen Datenarten und Quellen, hinsichtlich der Einbeziehung von Sekundärdaten, der Kontrolle der Verfahren und der geforderten Relevanz und Prognosegüte große Regelungsdefizite bestehen und neue Formen des Scoring, die über die klassische Bonitätsbewertung hinausgehen, nicht hinreichend abgedeckt sind (ausführlich Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein/GP Forschungsgruppe, Scoring nach der Datenschutz-Novelle 2009 und neue Entwicklungen, 2014, http://www.bmjv.de/SharedDocs/Downloads/DE/PDF/Scoring-Studie.pdf?__blob=publicationFile&v=3).

In Abs. 2 wird die Datenbeschaffung durch Auskunfteien in Bezug auf Bonitätsbewertungen mittels Scoring geregelt. Diese Regelung selbst beschränkt sich auf Scoringverfahren, in der Begründung ist aber generell von der Datenbeschaffung für **Kreditinformationssysteme** die Rede. Damit fallen Regelungsintention und Regelungsinhalt auseinander.

Zu § 32 Informationspflichten bei der Erhebung bei Betroffenen

Nach Abs. 1 Nr. 2 rechtfertigt schon ein „**unverhältnismäßiger Aufwand**“ den Verzicht auf Informationen nach Art. 13 DSGVO zur Verarbeitung bei einer Betroffenenerhebung. Diese äußerst unbestimmte Norm ermöglicht es Verantwortlichen, ohne weiteren Rechtfertigungsbedarf keine Betroffeneninformationen bereitzustellen. Die Schwelle zur Rechtfertigung fehlender Transparenz ist zu erhöhen.

Zu § 33 Informationspflichten bei Dritterhebung

Gemäß Abs. 1 Nr. 1 lit. a genügt schon eine **Gefährdung der ordnungsgemäßen Erfüllung der Aufgaben** einer öffentlichen Stelle, um auf eine Information der Betroffenen nach Art. 14 DSGVO zu verzichten. Dies ist eine unverhältnismäßige Beeinträchtigung des Transparenzanspruchs der Betroffenen. Angemessen wäre allenfalls eine höhere Schwelle, etwa die „Beeinträchtigung einer zulässigen Aufgabenerfüllung“.

Abs. 1 Nr. 2 lit. a legitimiert die Nichtinformation der Betroffenen, wenn eine erhebliche **Gefährdung der Geschäftszwecke** des Verantwortlichen angenommen wird. Dies eröffnet ein hohes Missbrauchspotenzial, da die Geschäftszwecke einseitig durch den Verantwortlichen definiert werden. Für eine angemessene Regelung bedürfte es ergänzender Schutzmaßnahmen. Die in Abs. 2 genannten Vorkehrungen, die zu „geeigneten Maßnahmen zur Information für die Öffentlichkeit“ verpflichten, genügen zur Verhinderung von Missbrauch der Transparenzausnahme nicht.

Zu § 34 Einschränkung des Auskunftsanspruchs

Abs. 1 Nr. 1 rechtfertigt die Auskunftsverweigerung bei Vorliegen eines Grundes zum Verzicht auf Informationen nach den § 33. Dies hat zur Folge, dass schon mit der **Gefährdung der Aufgabenerfüllung** oder der erheblichen Gefährdung der Geschäftszwecke die Auskunftsverweigerung begründet werden kann. Die Wahrung von angeblichen Geschäftsgeheimnissen, die in personenbezogenen Daten bestehen, können, anders als die Regelung suggeriert, eine Auskunftsverweigerung nicht rechtfertigen (ULD/GP Forschungsgruppe, Scoring-Gutachten, S. 44 ff. gegen BGH NJW 2014, 341). Diese Ausnahme von der Auskunftspflicht ist ersatzlos zu streichen. Angesichts des hohen Rangs des grundrechtlich in Art. 8 Abs. 2 S. 2 GRCh garantierten Anspruchs auf Auskunft – der Magna Charta des Datenschutzes (z. B. Mallmann in Simitis, BDSG, 8. Aufl. 2014, § 19 Rn. 1) – ist die Einschränkung des Auskunftsanspruchs unverhältnismäßig und verfassungswidrig.

Zu § 35 Einschränkung der Löschungsverpflichtung

Abs. 1 sieht vor, dass keine Löschpflicht besteht, wenn „eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit **unverhältnismäßigem Aufwand** möglich ist“. Diese Regelung steht im Widerspruch zu Art. 25, 32 DSGVO zu den technisch-organisatorischen Maßnahmen. Solche Maßnahmen zielen auch auf die Intervenierbarkeit von Daten ab, die bei der Gestaltung der Systeme beachtet werden muss. Automatisierte Verfahren, die in der Vergangenheit nicht in der Lage waren, spezifische Löschungen vorzunehmen, wurden inzwischen überarbeitet. Die Norm würde nun dazu einladen, Verfahren zu etablieren, mit denen mangels Löschbarkeit der Daten auf obligatorische Datenlöschungen verzichtet werden könnte.

Zu § 36 Einschränkung des Widerspruchsrechts

Nach der Regelung besteht kein Recht auf Widerspruch nach Art. 21 Abs. 1 DSGVO, „soweit an der Verarbeitung ein **zwingendes öffentliches Interesse** besteht, das die Interessen der betroffenen Person überwiegt oder eine Rechtsvorschrift zur Verarbeitung verpflich-

tet“. Diese Norm bringt das Recht, Widerspruch einzulegen und das Recht, auf der Grundlage eines Widerspruchs eine Veränderung bei der Datenverarbeitung zu bewirken, durcheinander. Ein Widerspruch ist für sich nicht in der Lage, einen Verarbeitungszweck ernsthaft zu beeinträchtigen; dies gilt allenfalls für die sich evtl. daraus ergebende Einschränkung der Verarbeitung. Die Regelung ist überflüssig und sollte gestrichen werden.

Zu § 37 Automatisierte Entscheidung über medizinische Entgelte

In Abs. 1 Nr. 2 und Abs. 2 ist vorgesehen, dass automatisierte Entscheidungen „auf der Anwendung verbindlicher **Entgeltregelungen für Heilbehandlungen**“ beruhen und dabei Gesundheitsdaten verarbeitet werden dürfen, wenn angemessene Sicherungsmaßnahmen vorgesehen sind. Diese insbesondere auf den Versicherungsbereich abzielende Norm ist in einem allgemeinen Datenschutzgesetz systemfremd.

Die Regelung ist insofern gefährlich, dass sie im Interesse der Kosteneffizient der Abrechnung von Heilbehandlungen den Betroffenen aufgibt, zur Wahrung ihrer Interessen aktiv zu werden, wozu viele Menschen kognitiv oder auch aus anderen Gründen nicht in der Lage sein werden. Zwar fordert die Regelung, dass bei antragsablehnenden Entscheidungen „angemessene Maßnahmen zur Wahrung der berechtigten Interessen der betroffenen Person“ getroffen werden müssen, doch sind diese möglichen Maßnahmen derart unbestimmt formuliert, dass die Regelung dazu führen kann, dass Patienten bei der Abrechnung medizinischer Leistungen über den Tisch gezogen werden. Eine Regelung der Automatisierung in diesem Bereich muss in einem speziellen Gesetz unter **konkreter Benennung der Sicherungsmaßnahmen** erfolgen. Dies gilt auch vor dem Hintergrund, dass die geplante Regelung Vorbild sein könnte für eine Vielzahl weiterer automatisierter Abrechnungsverfahren.

Zu § 38 Datenschutzbeauftragte nicht-öffentlicher Stellen

Es ist zu begrüßen, dass die **bewährte Normierung aus dem BDSG** zum Datenschutzbeauftragten in der Wirtschaft inhaltlich weitgehend übernommen werden soll. Immer noch sehr viele Unternehmensleitungen sind der Ansicht, dass sie sich nicht um die Umsetzung des Datenschutzes kümmern müssten, solange sie keinen Datenschutzbeauftragten zu bestellen haben. Diese Einstellung kann sich durch die deutlich gestiegenen Höchstgrenzen für Bußgelder im Lauf der Zeit wandeln. Durch die Beibehaltung der bisherigen Regelungen zur Bestellpflicht von Datenschutzbeauftragten wird eine präventive Umsetzung des Datenschutzes – die aus Betroffenensicht unbedingt erforderlich ist – gefördert.

Zu § 39 Akkreditierung von Zertifizierungsstellen

Die nationale Umsetzungsnorm zu den Art. 42, 43 DSGVO zur datenschutzrechtlichen Zertifizierung und zur Erteilung von Datenschutzgütesiegeln und -prüfzeichen beschränkt sich darauf, die zuständigen Aufsichtsbehörden in Bund und Ländern und die Deutsche Akkreditierungsstelle für die Erteilung der Befugnis, als Zertifizierungsstelle tätig zu werden, für zuständig zu erklären. Diese äußerst schlanke Regelung lässt praktisch alles hinsichtlich der Akkreditierung von Prüfstellen und der von diesen vorzunehmenden Zertifizierungen im **Unklaren**. Dies veranlasst die Aufsichtsbehörden und die Deutsche Akkreditierungsstelle, alles Wesentliche in eigener Verantwortung zu regeln. Dies ist äußerst unbefriedigend. Nötig sind insbesondere Regelungen, mit denen schon im Rahmen des Zertifizierungsverfahrens und nicht erst durch eine Intervention der zuständigen Aufsichtsbehörden die Qualität der Zertifizierungen gewährleistet wird. Ohne eine solche Qualitätssicherung können Zertifikate zur Umgehung des Datenschutzes und zum Vertuschen von Datenschutzverstößen missbraucht werden.

Zu § 42 Strafantragserfordernis

Zur Strafverfolgung von Datenschutzverstößen bedarf es nach Abs. 3 eines Antrags. Antragsberechtigt sollen sein „die betroffene Person, der Verantwortliche, die oder der Bundesbeauftragte und die Aufsichtsbehörde“. Damit sollen strafbare Datenschutzverstöße weiterhin kein Offizial-, sondern ein **Antragsdelikt** sein, was der gesellschaftlichen Bedeutung der Datenschutzdelikte nicht gerecht wird (Schulzki-Haddouti, Papiertiger, c´t 10/2016, 162 ff.).

Zu § 43 Verhängung von Geldbußen gegenüber öffentlichen Stellen

Abs. 2 sieht vor, dass gegen Behörden und **öffentliche Stellen des Bundes** keine Geldbußen verhängt werden. Mit der Regelung, die sich auf die Öffnungsklausel des Art. 83 Abs. 7 DSGVO beruft, werden öffentliche Stellen von Bußgeldverfahren vollständig freigestellt. Dies entspricht nicht den Intention der DSGVO und dem Ziel, die bestehenden Vollzugsdefizite durch verbesserte Sanktionen – im öffentlichen wie im nicht-öffentlichen Bereich – abzubauen.

Zu Teil 3 (§§ 45-84) Verarbeitung nach der JI-Richtlinie

Zu den Regelungsvorschläge der §§ 45 bis 84 wird aktuell keine Stellung genommen. Eine spätere Bewertung bleibt vorbehalten.

C Weitere gesetzliche Änderungen

Zu Artikel 2 Änderung des Bundesverfassungsschutzgesetzes

In § 13 Abs. 2 wird die Beschränkung der Verarbeitung (früher Sperrung) von Daten beim Bundesamt für Verfassungsschutz geregelt. Gemäß S. 2 genügt es für die **Verarbeitungsbeschränkung**, dass die Daten „mit einem entsprechenden Vermerk versehen“ werden. Dies gewährleistet nicht, dass keine weitere Nutzung dieser Daten erfolgt. Es muss sichergestellt werden, dass die verarbeitungsbeschränkten Daten den Nutzenden nicht mehr angezeigt werden und somit auch nicht unerkannt und evtl. gar unbewusst bei der Aufgabenwahrnehmung verwendet werden.

In § 26a Abs. 2 ist vorgesehen, die Datenschutzkontrolle der BfDI auszuschließen, „soweit die Einhaltung von Vorschriften der **Kontrolle durch die G 10-Kommission** unterliegt“. In der Vergangenheit hat sich gezeigt, dass

die Datenschutzkontrolle der bundesdeutschen Geheimdienste, anders als in der Begründung (S. 133) behauptet, unzureichend ist. Ein Grund hierfür liegt darin, dass die Tätigkeit der G-10-Kommission und die Kontrolle durch die BfDI sich gegenseitig ausschließen, obwohl in tatsächlicher wie auch in rechtlicher Hinsicht Überschneidungen bestehen. Die Kontrolle durch die G 10-Kommission und die der BfDI unterscheiden sich sowohl hinsichtlich der Methode wie auch der Fragestellung. Es ist daher gerechtfertigt, sich überschneidende Kontrollen zuzulassen. Hierdurch wird auch vermieden, dass z. B. durch Zuordnungsprobleme kontrollfreie Räume entstehen. Entgegen der Gesetzesbegründung ist die Regelung nicht geeignet, die bisher aufgetretenen Kontrolllücken zu beseitigen. Es ist nicht erkennbar, weshalb, wie in der Begründung aufgeführt, zwischen der G 10-Kommission und der BfDI konträre Ergebnisse entstehen können sollen. Selbst wenn dies der Fall wäre, bestünde insofern kein „Risiko", sondern allenfalls die Chance einer zweiten Meinung, zumal weder der BfDI noch der G 10-Kommission exekutive Durchgriffsrechte zugestanden werden.

In § 27 Abs. 1 ist vorgesehen, dass § 16 Abs. 1 des neuen BDSG nicht gelten soll, welcher der BfDI bei Feststellung von Datenschutzverstößen Untersuchungs- und Abhilfebefugnisse gemäß der DSGVO zugesteht, nachdem eine umfassende Anhörung stattgefunden hat. Es ist nicht erkennbar, weshalb diese Regelung, mit der die **Abstellung von Datenschutzverstößen** sicherstellen soll, für nicht anwendbar erklärt wird.

Zu Artikel 7 - Änderung des aktuellen Bundesdatenschutzgesetzes

§ 42b - Antrag der Aufsichtsbehörde auf gerichtliche Überprüfung von Angemessenheitsbeschlüssen der EU-Kommission

Es ist zu begrüßen, dass diese Regelung als eigenständige Änderung in das bisherige BDSG-alt eingefügt werden soll (siehe Art. 8 - Inkrafttreten/Außerkrafttreten) und am Tag nach der Verkündung dieses Gesetzes – und nicht erst am 25.05.2018 – in Kraft treten soll.

D Weiterer dringender Änderungsbedarf beim Datenschutzrecht

Der Entwurf behandelt einige Bereiche des Datenschutzes nicht, die dringend einer Regelung bedürfen.

Abgesehen von den schon genannten Themen des Beschäftigtendatenschutzes sowie des Datenschutzes im Bereich der Forschung gilt dies insbesondere für eine Regulierung der Auftragsdatenverarbeitung von Berufsgeheimnissen unterliegenden Verantwortlichen. **IT-Dienstleister**, die z. B. Anwalts- oder Arztpraxissysteme administrieren oder hochkomplexe IT-Systeme in Krankenhäusern oder medizinischen Laboren verwalten, genießen bisher nicht den in der StPO gesicherten Vertraulichkeitsschutz und unterliegen nicht der straf- und standesrechtlichen Schweigepflicht. Dies hat zur Folge, dass Berufsgeheimnisträger diesem Personenkreis bisher nach dem derzeit geltenden Recht keinen Zugang zu Patienten- oder Klientendaten gewähren dürfen. Dieses Defizit wird (noch nicht bzgl. des strafprozessualen Schutzes) durch einen Referentenentwurf eines „Gesetzes zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen", den das Bundesministerium für Justiz und Verbraucherschutz am 15.12.2016 vorlegte (teilweise) beseitigt. Es wird dringend geraten, diesen Entwurf beschleunigt zu bearbeiten und gemeinsam mit dem Umsetzungsgesetz zur DSGVO zu behandeln und zu verabschieden (http://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RefE_Neuregelung_Schutzes_von_Geheimnissen_bei_Mitwirkung_Dritter_an_der_Berufsausuebung_schweigepflichtiger_Personen.pdf;jsessionid=BB2D99E0FC070F2722D3C358448A65F6.1_cid324?__blob=publicationFile&v=1).

In der DSGVO und in der Folge auch im nationalen Umsetzungsgesetz besteht zudem ein großes datenschutzrechtliches Defizit darin, dass als Adressaten der Normen lediglich Verantwortliche und Auftragsverarbeiter benannt werden, nicht aber **Hersteller bzw. Anbieter von IT-Produkten** (Hard- und Software), mit denen personenbezogene Daten verarbeitet werden. Tatsächlich beruhen viele Gefährdungen und Beeinträchtigungen des Rechts auf informationelle Selbstbestimmung darauf, dass Verantwortliche oder Auftragsverarbeiter IT-Produkte einsetzen, die nicht den Anforderungen der DSGVO (z. B. der Art. 25, 32) genügen bzw. genügen können. In Ermangelung einer hinreichenden Kontrolle oder von technischen Einflussmöglichkeiten ist dies Verantwortlichen bzw. Auftragsverarbeitern oft nicht bewusst oder für diese nicht korrigierbar. Vorgegebene Verarbeitungsvorgänge, etwa in Form von Online-Formularen oder voreingestellten Datenweiterleitungen, sind oft weder hinreichend dokumentiert noch durch die (formalrechtlich verantwortlichen) Nutzenden beeinflussbar. Die ungenügende Umsetzung von Privacy by Default und Privacy by Design (vgl. auch Art. 25 DSGVO) oder generell unterlassene Maßnahmen zur Erhöhung der IT-Sicherheit durch die Hersteller führen oft dazu, dass nötige technisch-organisatorische Maßnahmen unterbleiben oder materiell-rechtliche Verstöße vorgegeben werden.

Ein modernes Datenschutzgesetz muss daher – ähnlich wie eine Adressierung von Straßenverkehrsvorschriften an die Kfz-Hersteller – auch die Hersteller und Anbieter von IT-Produkten, die der personenbezogenen Datenverarbeitung dienen, einbeziehen. Dies kann auch in der Form erfolgen, dass diesen, z. B. über Anforderungen an die Datenschutz-Folgenabschätzung, bestimmte **verpflichtende Datenschutzstandards** präventiv wirkend vorgegeben werden oder dadurch, dass diesen im Fall datenschutzwidriger Produkte Haftungsrisiken auferlegt werden. Die bisher vorgesehenen freiwilligen Zertifizierungen, die auf eine Selbstregulierung des Marktes setzen, genügen nicht, um die systematische Verbreitung von Datenschutzverstößen einzudämmen.

Dr. Thilo Weichert (Vorstandsmitglied der Deutschen Vereinigung für Datenschutz e.V.)

Frank Spaeing (Vorsitzender der Deutschen Vereinigung für Datenschutz e.V.)

Werner Hülsmann (stellv. Vorsitzender der Deutschen Vereinigung für Datenschutz e.V.)

Pressemitteilung der Deutschen Vereinigung für Datenschutz e. V. (DVD)

DVD: „Kein gläserner Zahlungsverkehr zwecks Terrorismusbekämpfung“

Presseerklärung vom 11.01.2017

Die Deutsche Vereinigung für Datenschutz (DVD) wendet sich gegen die Pläne der Europäischen Union, sämtliche Online-Finanztransaktionen nur noch nach Identifizierung des Kontoinhabers oder der Kontoinhaberin zuzulassen. Die Zahlung mit anonymen Prepaid-Karten am Point of Sale, also vor Ort im Geschäft, soll künftig nur noch bis maximal 150 € erlaubt sein, statt bisher 250 €. Dies ist in einer 5. Geldwäsche-Richtlinie vorgesehen, die von der EU-Kommission am 5. Juli 2016 vorgestellt und am 21. Dezember 2016 vom EU-Rat mit kleinen Änderungen bestätigt wurde. Begründet wird diese Initiative mit der Bekämpfung von Terrorismusfinanzierung und Geldwäsche.

Damit wird eine nach Ansicht der DVD nicht akzeptable Rundumüberwachung unschuldiger und unverdächtiger Menschen unter dem Vorwand der Bekämpfung des Terrorismus weiter vorangetrieben.

DVD-Vorstandsvorsitzender Frank Spaeing: „Nach dem Beschluss der Vorratsdatenspeicherung von Telekommunikationsdaten im Jahr 2015, nach dem Verbot anonymer SIM-Karten für die Mobilkommunikation und der geplanten massiven Ausweitung der Videoüberwachung im öffentlichen Raum wird mit der EU-Richtlinie die Ausleuchtung weiterer Aspekte unseres Alltagslebens vorangetrieben: Konsum und Zahlungsverkehr, welcher durch uns immer mehr digital und über das Internet erfolgt. Damit sind die Überwachungsbegehrlichkeiten noch nicht am Ende, wie wir aus Belgien wissen, wo die grenzüberschreitende Nutzung öffentlicher Verkehrsmittel nur noch zugelassen werden soll, nachdem man sich identifiziert hat. Politik, die meint, damit Terrorismus bekämpfen zu können, hat über dessen Ursachen wenig nachgedacht und ist blind für unsere Grundrechte“.

Der stellvertretende Vorsitzende der DVD, Werner Hülsmann, ergänzt: „Vor wenigen Tagen hat der Europäische Gerichtshof klargemacht, dass eine verdachtslose Totalüberwachung der Menschen grundrechtswidrig ist. Die vorgeschlagenen Maßnahmen sind Wasser auf die Mühlen von Terroristen, die unsere freiheitliche Gesellschaft in ein immer autoritäreres Fahrwasser treiben. Erschreckend ist, dass sich viele Politiker nicht nur in Berlin, sondern auch in Brüssel hierbei instrumentalisieren lassen.“

Die DVD fordert den umgehenden Stopp der weiteren Gesetzgebung und eine auf Fakten basierende rationale öffentliche Diskussion über die möglichen Maßnahmen zur Bekämpfung von Geldwäsche und Terrorfinanzierung.

Pressemitteilung des Netzwerks Datenschutzexpertise vom 11.01.2017

„Anonymität des elektronischen Zahlungsverkehrs muss erhalten bleiben“

Netzwerk Datenschutzexpertise fordert Gesetzgebungs-Stopp bei der 5. Geldwäsche-Richtlinie

Die 5. Geldwäsche-Richtlinie der Europäischen Union (EU) soll unter anderem anonyme Online-Zahlungen in der EU verbieten, die Grenze bei Transaktionen mit anonymen Prepaid-Karten auf 150 Euro herabsetzen und sämtliche Transaktionsdaten bei Finanzdienstleistern mindestens fünf Jahre speichern lassen. Die EU-Kommission will mit der vom Rat der EU am 21.12.2016 weitgehend bestätigten Richtlinie Geldwäsche und Terrorismusfinanzierung bekämpfen. Die Finanzdienstleister werden verpflichtet, die gespeicherten Transaktionsdaten bei Bedarf einer Finanzkontrollbehörde (Financial Intelligence Unit) bereitzustellen. Über den Aufbau eines Registers oder eines zentralen Datenabrufsystems, mit dem die Nutzer von Konten online identifiziert werden können, sollen die Zahlungen einzelnen Nutzern zugeordnet werden können.

Ein Gutachten des Netzwerks Datenschutzexpertise hierzu kommt zum Ergebnis, dass die Planungen gegen elementare Grundrechte auf Datenschutz, auf unbeobachtete Kommunikation und auf Eigentum verstoßen. Denn eine Verhältnismäßigkeitsprüfung – wie vom Europäischen Gerichtshof (EuGH) und



Bild: Adobe Stock

vom Bundesverfassungsgericht gefordert – wird nicht vorgenommen. Rechtliche oder prozedurale Vorkehrungen sind nicht vorgesehen. Undifferenziert sollen sämtliche elektronischen Zahlungsvorgänge mit einer Identifizierungspflicht belegt werden. Das Netzwerk Datenschutzexpertise fordert angesichts dieser Situation einen sofortigen Stopp der weiteren Gesetzgebung, eine umfassende Grundrechtsanalyse und eine intensive öffentliche Debatte über die Pläne.

Ute Bernhardt vom Netzwerk Datenschutzexpertise: „Nach der Vorratsdatenspeicherung von Fluggastdaten und den Kommunikations- und Bewegungsprofilen durch die Vorratsdatenspeicherung von Kommunikationsverbindungen sollen nun durch die Speicherung aller Daten von elektronischen Geldtransfers präzise Interessen-, Konsum- und Bewegungsprofile der gesamten EU-Bevölkerung gesammelt werden. Belege, dass Geldwäsche und Terrorismus über die Analyse von Bagatelltransfers aufgeklärt werden, gibt es nicht. Dafür ist klar, dass die EU-Kommission mit der neuen Richtlinie ihren im April 2016 beschlossenen „Gemeinsamen Rahmen für die Abwehr hybrider Bedrohungen“ umsetzt. Der formuliert das Ziel, nicht nur die Finanzierung des Terrorismus zu verfolgen, sondern auch die Finanzierung politischer „Interessengruppen oder Parteien am politischen Rand“. Die Geldwäsche-Richtlinie steht damit in einem viel größeren politischen Rahmen.“

Thilo Weichert vom Netzwerk Datenschutzexpertise: „Die Menschen haben einen generellen Anspruch auf Anonymität finanzieller Transaktionen. Dieses Recht darf nur eingeschränkt werden, wenn hierfür eine normenklare und verhältnismäßige Regelung besteht, die Vorkehrungen zum Schutz der Grundrechte enthält. In seinem jüngsten Urteil zur Vorratsdatenspeicherung von Telekommunikationsdaten vom 19.12.2016 hat der EuGH klar gemacht, dass eine anlasslose langfristige und undifferenzierte Speicherung von Daten über Alltagsaktivitäten unzulässig ist. Diese Ausführungen zur Telekommunikation lassen sich auf Finanztransaktionen übertragen. Das bisher unter dem Radar der öffentlichen Wahrnehmung durchgezogene Gesetzgebungsverfahren wurde initiiert, noch bevor die 4. Geldwäsche-Richtlinie in nationales Gesetz umgesetzt war und damit Erfahrungen gesammelt werden konnten. Es ist uns vollkommen unverständlich, dass dieses europarechts- und verfassungswidrige Vorhaben bisher weitgehend unbeanstandet den EU-Rat, den deutschen Bundesrat und die deutsche Bundesregierung passiert hat.“

Das ausführliche Gutachten des Netzwerks Datenschutzexpertise ist im Internet abzurufen unter:
http://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2016_5gwrl271216.pdf

Pressemitteilung der Deutschen Vereinigung für Datenschutz e. V. (DVD)

DVD zum Datenschutz-Kabinettsbeschluss: Keine Verwässung, sondern Umsetzung der Datenschutz-Grundverordnung ist nötig

Die Deutsche Vereinigung für Datenschutz e. V. (DVD) sieht gewaltigen Änderungsbedarf in Bezug auf den heute im Bundeskabinett beschlossenen Entwurf eines Umsetzungsgesetzes zur Europäischen Datenschutz-Grundverordnung, die im Mai 2016 in Kraft trat und vom 25.05.2018 an das bisherige Bundesdatenschutzgesetz (BDSG) ablöst.

Der Kabinettsbeschluss verkehrt dabei viele europäische Regelungen in ihr Gegenteil und lässt mit seinen Generalklauseln Anwender, Betroffene und Aufsichtsbehörden im Ungewissen. Er verstößt in einigen wesentlichen Punkten, etwa bei den Auskunfts- und Transparenzrechten der Betroffenen oder bei der Beeinträchtigung der unabhängigen Datenschutzkontrolle, gegen das in Artikel 8 der Europäischen Grundrechte-Charta garantierte Grundrecht auf Datenschutz.

Die Kritik der DVD bezieht sich u. a. auf folgende Punkte:

- Die geplante Regelung zur Videoüberwachung mit der Vorrangregelung für öffentliche Sicherheitsbelange ist europa- und verfassungswidrig.
- Die Regelung zur Bestellung der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) verstößt hinsichtlich der geforderten Transparenz und den personellen Anforderungen gegen die europarechtlichen Vorgaben.
- Die eingeschränkten Kontroll- und Sanktionsmöglichkeiten der BfDI im öffentlichen und insbesondere im Sicherheitsbereich untergraben insofern die Effektivität der Datenschutzaufsicht.
- Die Regelungen zur Vertretung der Aufsichtsbehörden der Länder im Europäischen Datenschutzausschuss beeinträchtigen deren Unabhängigkeit.
- Die Einschränkung der Kontrollbefugnisse der Datenschutzaufsicht im Bereich der Berufsgeheimnisse ist nicht akzeptabel.
- Die Möglichkeiten zur Verweigerung von Auskünften an Betroffene sind zu unbestimmt und zu weitgehend.
- Es verbleiben große Regelungsdefizite in Bezug auf die Datenverarbeitung in Beschäftigungsverhältnissen, der Forschung, der Beauftragung von IT-Dienstleistern sowie des Angebots von Herstellern und Anbietern von IT-Produkten.

Frank Spaeing, Vorsitzender der Deutschen Vereinigung für Datenschutz: „Es verwundert schon sehr, dass die Bundesregierung zunächst über Jahre hinweg eine verbindliche europäische Regelung bekämpfte, mit dem Argument, das hohe deutsche Datenschutzniveau dürfe nicht gesenkt werden, und nun, nachdem wir ein hohes europäisches Datenschutzniveau haben, alles tut, um dessen Niveau durch nationale Regelungen zu senken.“

Werner Hülsmann, stellv. Vorsitzender der DVD: „Der Kabinettsbeschluss ist wirtschafts-, fortschritts- und betroffenenfeindlich. Statt Rechtssicherheit zu schaffen, provoziert er bei allen Beteiligten Verunsicherung und Gesetzesverstöße. Deutschland darf nicht zum Bremser beim europäischen Datenschutz und zum schlechten Vorbild für andere Staaten werden.“

Thilo Weichert, Mitglied des DVD-Vorstands: „Der Entwurf verstößt gegen europäisches Recht und die deutsche Verfassung. Der Bundestag muss jetzt die Herkulesaufgabe bewältigen, aus einem verkorksten, rückwärtsgewandten Regierungsentwurf bis zum Ende der Legislaturperiode ein Gesetz zu machen, das den modernen Anforderungen des digitalen Grundrechtsschutzes genügt.“



Pressemitteilung der Deutschen Vereinigung für Datenschutz e. V. (DVD)

Datenschutzvereinigung begrüßt Vorgehen gegen „sprechende Puppe“

Am 17.02.2017 verkündete die Bundesnetzagentur, dass sie gegen die sprechende Kinderpuppe „Cayla“ vorgeht und diese aus dem Verkehr zu ziehen versucht. Sie rief Eltern auf, die „Puppe unschädlich (zu) machen“. Die Deutsche Vereinigung für Datenschutz e. V. (DVD) begrüßt diese Aktion: Der Schaden dieser Puppe besteht darin, dass unerkannt das im Raum gesprochene Wort erfasst und per funkfähige Sendeanlage an einen Provider gesendet wird, was nichts anderes ist als ein unerlaubter Lauschangriff nach § 201 Strafgesetzbuch und damit eine strafbare Spionage. Was mit den Aufzeichnungen passiert, weiß keiner der Nutzer.

Die Kinderpuppe ist aber nur ein derartiges Produkt; vergleichbar sind die Sprachassistenten, heißen sie nun Siri, Alexa, Cortana oder anders, wie sie in Smartphones, Computer, Lautsprecher oder Fernsehgeräten verbaut sind. Die Initiierung der Aufnahmen kann unabsichtlich erfolgen. Nicht eingeweihte Dritte werden derart in jedem Fall um Vertraulichkeitserwartungen betrogen. Die DVD erkennt, dass derartige „Helferlein“ bei korrekter Verwendung nützlich sein können, weist aber zugleich auf die damit verbundenen Gefahren hin: Ihr Einsatz setzt umfassende Informiertheit aller Anwesenden und echte Wahlfreiheit voraus. D.h. ist auch nur ein Gesprächspartner mit der Nutzung eines solchen Tools nicht einverstanden, dann muss es effektiv abgeschaltet werden.

DVD-Vorstandsmitglied Thilo Weichert: „In der Praxis haben wir derzeit noch einen gewaltigen Wildwuchs. Die Initiative der Bundesnetzagentur sollte ein Startschuss dafür sein, diesen einzuhegen. Unabdingbare Voraussetzung für Produkte mit akustisch initiierbarer Sprachübertragungen und -aufzeichnungen muss es sein, dass in der Produktbeschreibung der rechtliche Rahmen und die Risiken dargestellt werden und dass technisch-organisatorische Sicherungsmaßnahmen obligatorisch werden. Dazu gehört, dass allen räumlich Anwesenden technisch unzweideutig erkennbar gemacht wird, dass eine Sprachübertragung stattfindet.“

Der Vorsitzende der DVD Frank Spaeing ergänzt: „Für die Betroffenen ist nicht erkennbar, was mit derartigen Sprachaufzeichnungen passiert. In realistischen Fällen landen diese Informationen bei der US-amerikanischen NSA oder bei der heimischen Polizei. Effekt davon kann es sein, dass einem die Einreise in die USA verweigert wird oder plötzlich Strafverfolger zwecks einer Hausdurchsuchung vor der Tür stehen.“

Die Mitteilung der Bundesnetzagentur findet sich unter:

https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2017/14012017_cayla.html?nn=265778



Screenshot Webseite: http://myfriendcayla.de/


Screenshot YouTube-Werbevideo: https://www.youtube.com/watch?v=wa9npE9hsPw

Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

Puppe Cayla ist verbotenes Spionagewerkzeug

Eine blonde, blauäugige Puppe namens Cayla findet sich inzwischen in zahlreichen Kinderzimmern auch in Deutschland. Die Bundesnetzagentur hat jetzt festgestellt und bekannt gemacht, dass es sich dabei um eine „versteckte, sendefähige Anlage" handelt, weshalb sie Anfang des Jahres 2017 verschiedene Verkaufsstellen aufgefordert, Cayla aus dem Angebot zu nehmen. Wer sie bereits besitzt, soll sie vernichten oder professionell entsorgen. Weil der Besitz einer solchen Anlage strafbar ist, soll idealerweise der entsprechende „Vernichtungsnachweis" einer „Abfallwirtschaftsstation" an die Bundesnetzagentur geschickt werden. So können die Käufer nachweisen, dass sie nicht mehr im Besitz des Produkts sind.

My Friend Cayla ist ein Produkt des britischen Spielzeugherstellers Genesis und wird von der Firma Vivid vertrieben. Es ist ein Smart Toy, also ein Spielzeug, das sich mit dem Internet verbinden kann. Die Puppe verfügt über ein Mikrofon und einen Lautsprecher und kommuniziert über Bluetooth mit einer Smartphone-App. Leuchtet ihre Halskette, ist die Puppe online und Kinder können Fragen stellen, die Cayla anschließend versucht zu beantworten.

Im Dezember warnte die europäische Verbraucherschutzorganisation BEUC vor Cayla und ähnlichen Produkten: „Die mit dem Internet verbundenen Spielzeuge My Friend Cayla und i-Que (ein weiteres Produkt des Herstellers, Anm. d. Red.) scheitern grundsätzlich in Sachen Sicherheit und Datenschutz". So würden die aufgenommenen Spracheingaben nicht nur auf externen Servern gespeichert und zu Werbezwecken genutzt. Es sei denkbar, dass sich Unbefugte Zugriff auf die Mikrofone der Spielzeuge verschaffen.

Das fand unter anderem eine Untersuchung der norwegischen Verbraucherschutzbehörde Forbrukerradet heraus. In der Regel benötigt das erstmalige Verknüpfen zweier Bluetooth-Geräte (also etwa das Smartphone mit der Puppe) die Eingabe eines Sicherheitscodes. Im Fall von Cayla gibt es diese Überprüfung nicht. Jeder, der im Empfangsbereich der Puppe ist, kann sich somit über die App mit der Puppe verbinden. Anschließend sei es mit einem einfachen Trick möglich, das Mikrofon zu aktivieren – die Puppe würde somit zu einer Wanze werden.

Der deutsche Jura-Student Stefan Hessel von der Universität Saarbrücken überprüfte auf eigene Initiative in einem Rechtsgutachten, inwieweit es sich bei Cayla um eine nach § 90 Telekommunikationsgesetz (TKG) verbotene Sendeanlage handelt: „Die Puppe vermittelt für sich genommen den Eindruck, dass es sich um ein gewöhnliches Kinderspielzeug ohne technische Funktion handelt". Tatsächlich sei es aber möglich, auf das Mikrofon zuzugreifen, ohne dass die Puppe dies mit ihrem leuchtenden Schmuck anzeigt. Diese Sendeanlage würde „ihrer Form nach einen anderen Gegenstand vortäuschen" bzw. ist als ein „Gegenstand des täglichen Gebrauchs", weshalb die Einführung, der Besitz und die Verbreitung einer solchen Sendeanlage ist in Deutschland verboten sei.

Cayla, die seit zwei Jahren auf dem Markt war, erfüllt diese Voraussetzungen. Weil die Übertragung per Funk stattfindet, sei sie eine Sendeanlage. Weil es für Dritte nicht ohne weiteres erkenntlich ist, dass in ihrem Inneren ein Mikrofon steckt, liege eine Tarnung vor. Zudem sei sie zum heimlichen Abhören geeignet, auch wenn Hessel darauf hinweist, dass die Frage nach der Zweckbestimmtheit einen gewissen Interpretationsspielraum lässt.

Hessel legte seine Ergebnisse der Bundesnetzagentur vor: „Von dort bekam ich Rückmeldung, dass man meine Auffassung teilt, und die Puppe verboten ist". Am 24.01.2017 erklärte Jochen Homann, Präsident der Bundesnetzagentur: „Wer die sprechende Puppe Cayla kennt, weiß, dass diese Form der Alltagsspionage schon in die Kinderzimmer vorgedrungen ist." Deshalb versucht die Bundesnetzagentur jetzt, Cayla „aus dem Verkehr zu ziehen" und fordert die Besitzer auf, die Puppe zu zerstören. Es sei strafbar, eine getarnte Abhöranlage zu besitzen. Die Bundesnetzagentur bittet darum, den „Vernichtungsnachweis" auf ihrer Webseite anzufüllen, so ein Sprecher: „Wir haben aber nicht vor, Verwaltungsverfahren gegen Konsumenten zu starten. Staatsanwälte könnten allerdings aktiv werden, wie 10 Jahre zuvor wegen der „Teddycam", die in Plüschbären eingebaut war. Der Homeshopping-Sender, der sie vertrieb, musste einen Rückruf starten. Wer dem nicht folgte, wurde mit einer strafrechtlichen Ermittlung konfrontiert.

Der Hersteller Vivid widersprach der rechtlichen Bewertung: „My Friend Cayla verstößt in keiner Weise gegen Paragraph 90 TKG. Der verlangt, wie auch die Gesetzesbegründung klarstellt, für einen Verstoß neben anderen Voraussetzungen ausdrücklich, dass das betreffende Gerät in besonderer Weise dazu bestimmt ist, das nichtöffentlich gesprochene Wort unbemerkt abzuhören". Dies sei im Fall der Puppe nicht gegeben, die Auffassung der Bundesnetzagentur sei somit nicht haltbar. Es gebe keinen Grund, die Puppe zu zerstören weil es sich nicht um ein „Spionagegerät" handelt. Vivid will die Fragestellung „gerichtlich prüfen lassen".

Gebaut wird Cayla vom Unternehmen Genesis. Die Tonaufnahmen landen auf den Servern des US-Konzerns Nuance Communications. Der sammelt und analysiert millionenfach Stimmprofile als

„biometrische Fingerabdrücke“. Wird Cayla eine Frage gestellt, so sucht die Software eine Antwort und filtert „unanständige Worte“ aus. Nuance bietet seine Dienste auch dem Militär und Geheimdiensten an. Es ist zudem nicht nur die Sprachspionage, die aus Datenschutzsicht nicht akzeptabel ist. Gemäß IT-Anwalt Peter Hense fragt Caylas App „unglaublich viele Daten“ ab, inklusive Adressbuch des Smartphones. Es gibt keine Datenschutzerklärung, die auf die Spracherkennungsbiometrie hinweist.

Cayla ist nicht allein. 2015 gewann die Puppe „Hello Barbie“ von Mattell in Deutschland einen Big Brother Award (BBA). Der BBA-Negativpreis wird jährlich für Personen und Produkte verliehen, die gegen den Datenschutz verstoßen oder rücksichtslos Daten sammeln. Im Fall der Barbie-Puppe kritisierten die Datenschützer, dass alle Sprachaufnahmen an die Server eines Unternehmens weitergeleitet wurden (DANA 2/2015, 97). Anders als bei Barbie müssen die Kinder bei Cayla für das Gespräch keinen Knopf drücken und gedrückt halten. Der Sicherheitsforscher Linus Neumann sagte, Kinder würden somit schon von klein auf mit der Abschöpfung von Daten konfrontiert.

Ebenfalls 2015 sind Hacker in die Server des asiatischen Unternehmens VTech eingedrungen, das vernetztes Spielzeug und Lerncomputer herstellt. Dort fanden sie persönliche Daten von Kindern und Eltern sowie 190 Gigabyte Fotos und gespeicherte Chats. Die Hacker veröffentlichten die abgeschöpften Daten nicht. Der Angriff sollte bloß als Warnung dienen. Der Fall von VTech zeigte, dass Hersteller smarter Geräte offenbar nicht oder nur schlecht die Daten ihrer Nutzer schützen. In der Branche des Internet der Dinge (IoT) gibt es immer wieder Berichte über schlecht gesicherte Kameras und Haushaltsgeräte. Die Hersteller haben häufig andere Prioritäten als IT-Sicherheit oder Verschlüsselung. Es fehlt an Standards und Richtlinien, die es einzuhalten gilt.

Vor allem Eltern, die ihren Kindern Smart Toys kaufen, sollten stets genau auf die Sicherheitsvorkehrungen achten und die Datenschutzrichtlinien lesen. Sie sollten sich bewusst machen, dass die Daten – wenn schon nicht von Angreifern abgegriffen – dann doch zumindest an Server des Unternehmens übertragen werden könnten. Eine solche Puppe erfasst ja nicht nur die Gespräche mit dem Kind, sondern auch die der Eltern (Kühl, My Friend Cayla: Vernichten Sie diese Puppe, www.zeit.de 17.02.2017; Brühl, Die Spionin, SZ 18./19.02.2017, 12).

Bund

„Gesellschaft für Freiheitsrechte“ gegründet

JuristInnen und BürgerrechtlerInnen haben die „Gesellschaft für Freiheitsrechte“ (GFF, www.freiheitsrechte.org) gegründet, die sich in den Bereichen Privatsphäre, Datenschutz und Informationsfreiheit für die Grundrechte der Menschen einsetzen möchte.

Ulf Buermeyer, Richter am Landgericht Berlin und bekannt als Verteidiger von Bürgerrechten, hat sich mit weiteren MitstreiterInnen, z. B. auch den langjährigen Grünenpolitiker Malte Spitz, zusammengetan, um künftig Klagen zur Stärkung der Grundrechte in den Bereichen Privatsphäre, Datenschutz, Informations- und Pressefreiheit zu organisieren. Buermeyer spricht in dem Zusammenhang von „Verfassungspatriotismus“.

Die Organisation von Klagen, ohne selbst Kläger zu sein, also „strategisches Klagen“, ist für Deutschland bisher eher ungewöhnlich. In Amerika ist dieses Vorgehen verbreitet, bekannt durch Organisationen wie die American Civil Liberties Union, eine Bürgerrechtsorganisation. Ähnlich wie das amerikanische Vorbild wird die GFF die Kosten der Kläger decken, aber kein Geld dafür bezahlen, dass eine Klage entsteht. Buermeyer nennt das Prinzip „eine Rechtschutzversicherung für das Grundgesetz“. Man stelle sicher, dass Expertise und Geld vorhanden seien, um die „Freiheitsrechte zu verteidigen.“ Zur Expertise gehört auch, dass die JuristInnen explizit „bessere Klagen“ zusammenstellen wollen. Es geht also nicht darum, Karlsruhe zu überlasten, sondern mit klug formulierten Klagen Politik zugunsten der BürgerInnen zu beeinflussen. Bei der GFF verspricht man sich, eine gewisse Nachdenklichkeit in den Parlamenten auszulösen, die sich mit entsprechenden Gesetzen befassen. Sie soll sich einstellen, wenn die ersten Gesetze vom Bundesverfassungsgericht nach entsprechenden Klagen aus den Angeln gehoben wurden.

Zu den ersten Fällen der GFF gehört eine Verfassungsbeschwerde gegen das neue BND-Gesetz; außerdem unterstützt die Gesellschaft bereits Transparenzklagen nach dem Informationsfreiheitsgesetz, was dafür sorgen soll, dass BürgerInnen und JournalistInnen problemloser an öffentliche Informationen gelangen können. Wenigstens jetzt, zu Beginn der Arbeit, will sich die Gesellschaft ausschließlich um staatliche Attacken auf die Grundrechte kümmern. Private Akteure, wie Google oder Facebook, stehen für die GFF vorläufig nicht im Fokus.

Unter den einfachen Mitgliedern der GFF, die sich aus Spenden finanzieren soll, finden sich weitere bekannte Juristen und Aktivisten. Eng verwoben ist der Verein zum Beispiel mit netzpolitik.org, der Internetseite, auf der seit Jahren kompetent über die Verletzung digitaler Bürgerrechte berichtet wird. Der Gründer von Netzpolitik, Markus Beckedahl, ist Mitglied der GFF. Weitere Partner sind Amnesty International, der Chaos Computer Club und Reporter ohne Grenzen (Boie, Aus Liebe zum Grundgesetz, SZ 11.11.2016, 12).

Bund

Arne Schlatmann ist erster Geheimdienstbeauftragter

Der Jurist Arne Schlatmann, 52, wird der erste Geheimdienstbeauftragte des Bundestages. Am 14.12.2016 haben ihn die SPD- und Unions-Mitglieder im Gremium dazu gewählt, am 10.01.2017 hat er das neu geschaffene Amt für fünf Jahre angetreten. Seine Aufgabe besteht in der stetigen hauptamtlichen Kontrolle der Geheimdienste des Bundes. Er soll dafür einen Stab von 20 Mitarbeitern bekommen und den Abgeordneten im Parlamentarischen Kontroll-Gremium des Bundestages zuarbeiten.

Die Opposition hätte dafür gern einen Richter berufen, einen unabhängigen Geist mit klarer Distanz zum Sicherheitsapparat. Dem entspricht das CDU-

Mitglieds Schlatmann eher nicht. In 23 Berufsjahren hat er fast nie das Bundesinnenministerium verlassen. Er war im Leitungsstab bei den Ministern Schäuble und de Maizière, dann Büroleiter bei Hans-Peter Friedrich. Der heutige Chef des Bundesnachrichtendienstes Bruno Kahl war einst sein Vorgesetzter. Der heutige Chef des Bundesamts für Verfassungsschutz Hans-Georg Maaßen war lange sein Kollege.

Schlatmann soll sich einen Ruf als gründlicher Arbeiter erworben haben, der keine Profilierung sucht. Lange betreute er das Thema Verwaltungsverfahrensrecht. Schlatmann will die Arbeit der Geheimdienste, so sagt er, konstruktiv begleiten: Wenn sich an irgendeiner Stelle zeigen sollte, dass es ihnen an Geld oder Befugnissen fehle, dann seien auch dies Missstände, für deren Behebung sich ein Kontrolleur einsetzen könne (Steinke, Arne Schlatmann, SZ 16.12.2016, 4).

Bund

Zunehmend Verbraucherbeschwerden bei Telefonwerbung

Die Bundesnetzagentur, die oberste Aufsichtsbehörde über den Telekommunikationsmarkt in Bonn, verzeichnete 2016 mehr Kundenbeschwerden als je zuvor, wobei unerlaubte Telefonwerbung eine große Rolle spielte. Im Jahr 2016 sind pro Monat im Schnitt 18.000 Verbraucheranfragen und -beschwerden eingegangen und damit erstmalig im Jahr auf 220.000 gestiegen (2015: 200.000). Rund 3.000 Telefonnummern wurden wegen unerlaubter Werbung abgeschaltet und Bußgelder von mehr als 800.000 € verhängt. Der Präsident der Bundesnetzagentur Jochen Homann erklärte: „Wir nutzen unsere Befugnisse konsequent aus". Verbesserungen registrierte die Behörde 2016 beim Anbieterwechsel. In 2.700 Fälle habe sich die Bundesnetzagentur eingeschaltet, weil es bei einem Wechsel zur Versorgungsunterbrechung gekommen war. Ein Jahr zuvor lag die Zahl noch doppelt so hoch (Kramer, Mehr Verbraucherbeschwerden bei Bundesnetzagentur 2016, www.heise.de 28.12.2016).

Bund

Initiative zur Vereinfachung von Datenschutzerklärungen

Das Bundesministerium für Justiz und Verbraucherschutz (BMJV) und der Online-Modehändler Zalando haben ein Werkzeug entwickelt, mit dem Betreiber von Webseiten kurze, verständliche Zusammenfassungen von komplizierten Datenschutzbestimmungen erstellen können. Sie stellten das Programm auf dem IT-Gipfel in Saarbrücken am 16.11.2016 vor. Die aktuellen Datenschutzbestimmungen von Amazon.de sind sieben Seiten lang, die der Partnervermittlung Parship acht Seiten, bei Facebook Deutschland sind es zehn Seiten. Das BMJV hatte zunächst ein Jahr zuvor eine Initiative zusammen mit Verbraucherschützern und IT-Unternehmen gestartet. Damit sollten Webseiten den Nutzenden die Regeln zum Datenschutz auf einer einzigen Seite verständlich zusammengefasst werden. Dieser sogenannte One-Pager ist zwar nicht rechtlich bindend, so dass irgendwo weiterhin auf den langen Text verlinkt sein müsste, den kaum jemand liest. Doch erhalten die Nutzenden darüber einen Überblick, worauf sie sich mit einer Registrierung auf einem bestimmten Portal einlassen. Auf der Website des BMJV gibt es eine Vorlage für einen solchen One-Pager.

Die Beteiligten stellten allerdings bald fest, dass kaum eine Internetseite die Vorlage nutzt und fast überall weiterhin nur die viel zu langen Juristentexte zu finden sind. Zalando beispielsweise hat die Information zwar mit bunten Balken in viele Abschnitte aufgeteilt. Das sieht nicht mehr ganz so furchtbar aus, macht den Text aber nicht kürzer. Justizminister Maas und der Zalando-Manager Philipp Erler stellten nun eine Plattform vor, mit der die Betreiber von Internetseiten die einseitige Zusammenfassung mit wenigen Klicks erstellen können, auch ohne Hilfe von JuristInnen oder WebdesignerInnen. Dabei wird etwa abgefragt, ob die Website Google Analytics nutzt und ob die Daten verschlüsselt übertragen werden. Eine Software stellt daraus die Übersicht zusammen. In wenigen kurzen, mit Bildern versehenen Absätzen sollen die Nutzenden darauf sehen können, welche Daten sie preisgeben und was damit geschieht. Erler von Zalando erläuterte: „Es gibt immer noch ein großes Misstrauen gegenüber E-Commerce, die Nutzer haben Angst und sind zugleich uninformiert."

Dies bestätigte eine Umfrage des IT-Branchenverbandes Bitcom im Jahr 2015. Zwei Drittel der Befragten erklärten, sie hätten Angst „die Kontrolle über den Schutz meiner Privatsphäre zu verlieren". In der Praxis setzen Menschen jedoch meist schnell einen Haken bei „Ich stimme den Datenschutzbedingungen zu" und klicken weiter. Nur 14% gaben in derselben Umfrage an, sie läsen die Erklärungen bis zum Ende durch. Mit dem neuen Werkzeug hofft man nun, den Nutzenden die nötigen Informationen besser zugänglich zu machen. Florian Glatzner vom Verbraucherzentrale Bundesverband findet die Initiative gut: „Alles was hilft, Datenschutz besser verständlich zu machen, ist erst mal positiv." Das Software-Werkzeug wird allen Betreibern von Websites kostenlos zur Verfügung gestellt. Auch der Mitinitiator Zalando, so Erler, will eine solche Zusammenfassung verwenden (Endt, Mach´s kurz, SZ 16.11.2016, 26).

Bund

KBA-Punktekonto von Betroffenen online abrufbar

AutofahrerInnen können seit dem 08.12.2016 ihre Punkte in Flensburg online auf der Homepage des Kraftfahrt-Bundesamtes (KBA) in Flensburg kostenfrei abrufen. Dafür benötigen sie einen der neuen Personalausweise mit freigeschalteter Online-Funktion, eine AusweisApp auf dem eigenen Computer und ein Kartenlesegerät. Verkehrsminister Alexander Dobrindt (CSU) erklärte: „Wir digitalisieren die Verwaltung. Das spart Zeit und Geld" (Punkte in Flensburg online abrufbar, www.heise.de 08.12.2016).

Bundesweit

Polizei kommuniziert mit TK-Unternehmen unverschlüsselt und rechtswidrig

Viele E-Mail-Anbieter stellen inzwischen sog. Transparenzberichte ins Netz, in denen die Öffentlichkeit informiert wird, in welchem Umfang und auf welcher Rechtsgrundlage Behörden Kundendaten angefordert haben. Diese beschränken sich meistens auf knappe Zahlen mit begrenzter Aussagekraft. Der Anbieter Posteo geht über bloße Statistiken hinaus und veröffentlicht sogar eine Auswahl konkreter Behördenanfragen. Diese teils geschwärzten Dokumente offenbaren, dass die Polizei bei ihren Auskunftsersuchen bei etwa der Hälfte aller Ersuchen rechtswidrig vorgehen.

Diese Behördenanfragen werden in großem Umfang per E-Mail gestellt. Darin enthalten sind sensible personenbezogene Informationen wie E-Mail-Adressen, Aktenzeichen und Tatvorwürfe. Auch im Jahr 2016 waren alle bei Posteo eingehenden Mails unverschlüsselt und damit während des Übermittlungsvorgangs unsicher und mitlesbar. Die Polizei vieler Bundesländern selbst verstößt so gegen Datenschutzgesetze, die eine Verschlüsselung zwingend vorschreiben.

Ein Polizist aus Mecklenburg-Vorpommern schickte gar einmal ein Auskunftsersuchen von einer offensichtlich privaten E-Mail-Adresse, die auf „online.de" endet, und gab diese sogar in seiner offiziellen Signatur an. Das eingeschaltete Landesinnenministerium konnte den Fall bislang nicht aufklären. Ein großer deutscher E-Mail-Anbieter bestätigte, dass dort immer noch schätzungsweise zehn Prozent der Kommunikation mit den Ermittlungsbehörden über unverschlüsselte E-Mails geführt werde.

Beamten fordern oft Daten an, ohne die Rechtsgrundlage zu benennen, wie es ausdrücklich im Gesetz vorgeschrieben ist. Oder sie nennen eine falsche, verwechseln etwa das Telekommunikationsgesetz mit dem Telemediengesetz. Der Berliner E-Mail-Anbieter mailbox.org bestätigt, dass etwa die Hälfte aller Anfragen Fehler enthielten. Oft werden keine Muster oder Standards verwendet und Auskunftsersuchen frei formuliert.

Ein wichtiger rechtlicher Unterschied ist der zwischen Bestands- und Verkehrsdaten. Die weitaus meisten Anfragen betreffen Bestandsdaten, das sind etwa Name, Adresse und Bankverbindung eines Kunden. Sie dürfen schon beim Verdacht auf eine bloße Ordnungswidrigkeit abgefragt werden. (Dies jedoch unergiebig, wenn der E-Mail-Anbieter wie etwa Posteo gar keine Bestandsdaten speichert.) Verkehrsdaten sind die Angaben darüber, wann und an wen jemand eine E-Mail verschickt hat und wann er eingeloggt war. Sie dürfen nur bei Verdacht auf eine schwere Straftat abgefragt werden oder wenn die Straftat mittels Telekommunikation begangen wurde; die Behörden brauchen dafür eine richterliche Genehmigung. In der Praxis versuchen Polizisten es trotzdem immer wieder ohne.

Im Rahmen einer Bestandsdatenabfrage forderte etwa eine Kriminalkommissarin des Bundeskriminalamtes (BKA) wie selbstverständlich „die letzten Login-Daten" an. Das BKA erklärte diesen Vorgang zu einem „bedauerlichen Einzelfall", was von Posteo bestritten wird: „Bisher haben uns insgesamt sechs Bestandsdaten-Ersuchen des BKA erreicht. Fünf waren nicht korrekt. In drei Fällen wurde nach Verkehrsdaten gefragt."

Einmal bat ein Polizist aus Mecklenburg-Vorpommern gar um Informationen zu „weiteren Anfragen durch Ermittlungsbehörden (event. Aktenzeichen dieser)". Ein anderer aus Sachsen begehrte eine Verkehrsdatenauskunft und kreuzte in seinem Formular an: „Ein richterlicher Beschluss liegt z. Z. noch nicht vor." Doch die Diensteanbieter müssen jedes Gesuch prüfen. Sie unterliegen selbst engen Bestimmungen. Gäben sie tatsächlich Verkehrsdaten ohne richterlichen Beschluss heraus, machten sie sich wegen Verletzung des Fernmeldegeheimnisses strafbar. Peer Heinlein, Geschäftsführer von mailbox.org, sagt: „Das könnte man juristisch sogar als Anstiftung zur Straftat verstehen."

Posteo hat viele Fälle bereits an die Landesdatenschutzbeauftragten weitergeleitet. Vor allem das Problem der unverschlüsselten Kommunikation durch die Polizei ist vielen von ihnen seit langem bekannt. In Bayern wird das Thema demnach „regelmäßig erörtert" und ist „immer wieder Anlass für datenschutzrechtliche Überprüfungen". Die Datenschutzbehörde für Niedersachsen berichtet von „Sensibilisierungsmaßnahmen" in betroffenen Behörden. Sein sächsischer Kollege setzte dem Landespolizeipräsidenten Anfang 2015 eine Frist, „mir mitzuteilen, welche Abhilfemaßnahmen er ergriffen hat". Der Polizeipräsident reagierte mit einem ziemlich komplizierten Erlass an alle Polizeidienststellen. Er trägt den herrlich bürokratischen Titel: „Grundsätzliche Maßnahmen zur Gewährleistung des Schutzes personenbezogener Daten im Rahmen der polizeilichen elektronischen Kommunikation."

Eine Reaktion des Innenministeriums von Baden-Württemberg zeigt, wie groß der Aufklärungsbedarf bei den Behörden ist. Auf die Frage, warum auch Polizisten aus diesem Bundesland unverschlüsselte Mails senden, teilte es mit, es bestehe „die technische Problematik", dass das von Posteo bereitgestellte „spezielle Verschlüsselungsverfahren" nur mit gebührenpflichtiger Software genutzt werden könne. Als wäre für rechtmäßiges Verhalten Voraussetzung, dass dies keine Kosten verursacht. Die Antwort ist zudem falsch, da Posteo zwei weitverbreitete Verfahren anbietet, von denen eines (GnuPG/PGP) komplett kostenlos genutzt werden kann. Das Bundesamt für Sicherheit in der Informationstechnik empfiehlt es in seinem Grundschutzkatalog. Für das andere Verfahren ist lediglich ein Zertifikat einer vertrauenswürdigen Zertifizierungsstelle nötig, das 20 bis 50 € im Jahr kostet.

Kommunikationssicherheit etabliert sich nur sehr langsam in der Verwaltung und in Deutschlands Polizeidienststellen. Die Berliner Polizei hat nach eigenen Angaben erst im dritten Quartal vergangenen Jahres „eine Verschlüsselungsinfrastruktur eingeführt". Mit ihr sollen alle künftigen polizeilichen Anfragen gesichert werden. Baden-Württemberg richtet derzeit eine Zentralstelle ein, die landesweit die Technik für sichere Datenabfragen bereitstellen soll. Die Testphase läuft bereits, der Betrieb soll in Kürze aufgenommen werden. Da mit der Zentralstelle auch die Abfrageverfahren vereinheitlicht werden, soll es nicht mehr vorkommen, dass Polizisten bei Auskunftsersuchen über den gesetzlich zulässigen Rahmen hinausschießen. Dies würde nicht nur mehr Datensicherheit ge-

währleisten, ohne dass die Ermittlungsverfahren verzögert werden, sondern zugleich die Anbieter von E-Mail-Diensten entlasten, die einen hohen Kosten, Personal- und Zeitaufwand wegen der Bearbeitung fehlerhafter Anfragen und ständiger Auseinandersetzung mit Behörden haben. Posteo-Mitgründerin Sabrina Löhr meinte: „Dass uns regelmäßig hohe Anwaltskosten entstehen, weil wir uns rechtskonform verhalten, ist absurd“ (Tomik, Behördliche Abfragen: Wie dilettantisch ‚Polizisten mit sensiblen Daten umgehen, www.faz.net 18.01.2017).

Bundesweit

Elektronische Fußfessel für mutmaßliche Islamisten?

Elektronische Fußfesseln sind seit fünf Jahren im Einsatz gegen Schwerkriminelle. In Deutschland wurden seit 2012 insgesamt 138 verurteilte Sexualstraftäter und Gewaltverbrecher per GPS überwacht. Nach dem Willen der hessischen Justizministerin Eva Kühne-Hörmann (CDU) sollen künftig auch islamistische Gefährder mit der 24-Stunden-Überwachung belegt werden. Die Politikerin sieht den Einsatz der Fußfessel als „wichtige(n) Baustein für mehr Sicherheit in Deutschland“. So könne beispielsweise sichergestellt werden, dass „szenebekannte Hassprediger bestimmte Moscheen nicht mehr betreten oder dass sich einschlägig Verurteilte extremistische Straftäter bestimmten kritischen Infrastrukturen wie Kraftwerken, Bahnhöfen oder Flughäfen nicht nähern dürfen.“

Aktuell ist die Überwachung der bekannten rechten, linken oder islamistischen Gefährder auf Grundlage des Fußfessel-Gesetzes nicht möglich. Per Fußfessel dürfen derzeit gefährliche Straftäter überwacht werden, für die die sogenannte Führungsaufsicht nach der eigentlichen Haftstrafe angeordnet wurde. Wer unter Führungsaufsicht steht, kann Geboten und Verboten unterworfen werden; zum Beispiel kann ein Pädophiler die Auflage erhalten, sich von Kinderspielplätzen fernhalten zu müssen. Seit 2012 kann die Einhaltung dieser Auflagen per elektronischer Fußfessel kontrolliert werden.

Das Bundesland Hessen leitet die „Gemeinsame Überwachungsstelle der Länder“ (GÜL) und ist somit auch für die Umsetzung der Überwachung per elektronischer Fußfessel zuständig. Zum Jahreswechsel 2016/2017 wurden 88 Personen von der GÜL überwacht, 63 wegen eines Sexualdelikts, 25 wegen einer vorausgegangenen Gewalttat. Die Vorgaben für eine Überwachung sind streng und eng an das bestehende Gesetz geknüpft. Die Justizministerin Kühne-Hörmann steht ihrer Forderung nach einer Ausweitung der elektronischen Fußfessel nicht allein da: Die Experten-Gruppe der Justizminister der Länder hat sich ebenfalls dafür ausgesprochen, die Überwachung auf „terrorverdächtige Extremisten“ auszuweiten (Elektronische Fußfessel für mutmaßliche Islamisten? www.chiemgau24.de 02.01.2017; Elektronische Fußfesseln, SZ 03.01.2016, 5).

Bundesweit

CDU fordert verschärfte Sicherheitsmaßnahmen gegen Terrorismus

Saarlands Innenminister und stellvertretender Vorsitzender der Innenministerkonferenz Klaus Bouillon (CDU) fordert den Einsatz modernster Gesichtserkennungssoftware bei der Videoüberwachung öffentlicher Plätze. Im Kampf gegen Terrorismus und organisiertes Verbrechen müssten dafür gesetzliche Grundlagen geschaffen werden: „Wenn wir eine Liste mit den meistgesuchten Verbrechern der Welt haben, potenziellen Mördern, dann möge mir einer erklären, warum ich die biometrische Gesichtserkennung nicht einsetzen sollte.“ Beim Einsatz von Videoüberwachung mit biometrischer Gesichtserkennung „laufen da Hunderttausende Leute vorbei und das interessiert die Kamera überhaupt nicht“. Die Gesichtserkennung per Computer, für die auch Bundesinnenminister Thomas de Maizière plädiert, ist politisch umstritten. Bouillon zeigte sich „fest überzeugt“, dass auch die Gesichtserkennung „in den nächsten Wochen unter dem Druck der Ereignisse irgendwann „unstrittig werden“ könne.

Er glaube nicht, dass die Diskussion um die von De Maizière vorgeschlagene Übernahme der Verfassungsschutzaufgaben in die Bundesverwaltung beendet sei. Besonders kategorisch hatte Bayern betont, am freistaatlichen Verfassungsschutz festzuhalten. Bouillon: „Man kann ja das eine tun, ohne das andere zu lassen. Die Kompetenzverteilung wird ein Thema bleiben.“ Die Zusammenarbeit zwischen Bundeskriminalamt und Landeskriminalämtern habe sich in jüngster Vergangenheit „wesentlich verbessert“. Auch für den Verfassungsschutz gelte, dass man „eine deutlich bessere Kooperation als bisher“ brauche. Es gebe Möglichkeiten zur Zusammenarbeit ohne Aufgabe der Selbstständigkeit der Länder: „Vom Grundsatz her hat De Maizière absolut recht.“

Bouillon begrüßte, dass die Bundesregierung sich am 10.01.2017 auf die Einführung einer elektronischen Fußfessel für Gefährder, die leichtere Inhaftierung von Gefährdern im Rahmen der Abschiebehaft und des Ausreisegewahrsams und eine Residenzpflicht für Asylbewerber, die ihre Identität verschleiern, einigte: „Wir müssen ja versuchen, die Leute unter Kontrolle zu bringen, soweit das geht. Das sind doch zum Teil potenzielle Zeitbomben“ (Saar-Innenminister dringt auf biometrische Videoüberwachung, www.swp.de 12.01.2017).

Bundesweit

Fußballfan-Erfassung in SKB-Dateien

Durch intensives Nachhaken von Wiebke K. wegen eines polizeilichen „Betretens- und Aufenthaltsverbots“ in Bezug auf ein Auswärtsspiel des Fußballvereins Hannover 96 in Braunschweig im Frühjahr 2014 kam heraus, dass die Polizei heimlich, still und leise einen neuen Typ Polizeiregister eingeführt hatte – die SKB-Dateien. SKB steht für „szenekundige Beamte“. PolizistInnen, die Fußballfans begleiten, tragen dort Personen ein, die sie im Stadionumfeld fotografiert, deren Personalien sie erfasst oder anderweitig ermittelt haben. Es kommt dabei nicht darauf an, ob die Ermittlungen zu einer Anklage geführt haben. Die SKB-Daten werden

zwischen den Dienststellen in Deutschland ausgetauscht. Erfasst sind in diesen Dateien bundesweit einige Tausend Fußballfans – i. d. R. ohne dass diese dies wissen. Die Erfassung der Ultras in den SKB-Dateien ist ein Teil eines größeren Bildes in der schon Jahre andauernden Auseinandersetzung der Polizei mit teilweise gewaltbereiten, Schlägereien durchführenden rivalisierenden Fangruppen. Derartige Ultras gibt es in Deutschland geschätzt etwa 10.000.

Die Gewalt bei Fußballspielen wird in der jährlichen Statistik der Zentralen Informationsstelle Sporteinsätze (ZIS) der Polizei erfasst. Die ZIS-Statistik listet auf, was an Störungen über eine Saison hinweg zusammenkommt. Gemäß Zahlen von Oktober 2016 wurden in der vergangenen Saison Fans 13.467 Mal festgesetzt und 7.773 Strafverfahren eingeleitet. 1.265 Personen wurden verletzt. Die Zahl der ausgesprochenen Stadionverbote sank gegenüber der Vorsaison von 1.203 auf 829. Die Zahl der Ermittlungsverfahren wegen des Verstoßes gegen das Sprengstoffgesetz – dabei geht es um das Abbrennen von Bengalos und Rauchtöpfen sowie das Abfeuern von Raketen – reduzierte sich um über ein Drittel auf 566 Fälle. Angestiegen ist dagegen die Zahl der Festnahmen. Diese gegenläufige Entwicklung bringt Rechtsanwalt Andreas Hüttl, an den sich Mitglieder der deutschen Fanhilfen wenden, wenn sie Ärger mit der Polizei haben, zu der Feststellung: „Während die Gewalttaten im Umfeld der Stadien abgenommen haben, haben die repressiven Maßnahmen immer weiter zugenommen."

Hüttl vertritt Wiebke K. vor Gericht. Die 27jährige Rechtsanwaltsgehilfin ist seit 14 Jahren Anhängerin von Hannover 96. In erster Instanz konnten sie erreichen, dass einige Eintragungen von ihr in der SKB-Datei gestrichen wurden, z. B. ein eingestelltes Ermittlungsverfahren, von dem Wiebke K. nie etwas erfahren hatte. In Niedersachsen wurden die gesetzlichen Anforderungen an diese Polizeidateien erst nachträglich erfüllt, nachdem gegen eine SKB-Datei geklagt wurde. In Hamburg leugnete die Polizei noch im Jahr 2014 die Existenz einer SKB-Datei. Durch eine parlamentarische Anfrage einer Linken-Abgeordneten Anfang 2016 kam dann heraus, dass dort eine solche Datei existiert mit mehr als 1.000 Fans des HSV und 400 St.-Pauli-Fans. Angelegt wurde die Datei am 01.06.2006, wenige Tage vor Beginn der Fußballweltmeisterschaft in Deutschland. Nachdem die Existenz dieser Datei bekannt war, blieb der Polizei in Hamburg nichts anderes übrig, als sie komplett zu überarbeiten und einige Hundert Fans zu streichen.

Thüringen führt, so das dortige Innenministerium, aus Gründen des Datenschutzes keine eigene SKB-Datei. Doch möchte man, so Innen-Staatssekretär Udo Götze auf eine Linken-Anfrage, die Daten anderer Bundesländer nutzen: „Ich gehe davon aus, dass die anderen Bundesländer datenschutzkonform arbeiten und diese Anfragen dann unproblematisch möglich sind."

In Nordrhein-Westfalen wollen Ende 2016 einige Hundert Ultras von der Polizei wissen, was über sie gespeichert ist. Dort ist das Verhältnis zwischen Fans und Polizei besonders angespannt. Vor einiger Zeit hat die Polizei in Düsseldorf DNA-Proben von zwei Anhängern genommen – wie sie sagt, auf freiwilliger Basis. Damit sollten künftig Straftaten aufgeklärt werden – als Teil des Konzepts „Intensivtäter Sport". Eine Fangruppierung wies darauf hin, dass die involvierten Ultras strafrechtlich nicht verurteilt sind und kommentierte: „Von einer Entnahme auf freiwilliger Basis kann dabei nicht gesprochen werden. Entweder die Probe wird abgegeben, oder die Betroffenen erwartet eine härtere Gangart." Es ist ein Fall bekannt, in dem eine DNA-Analyse im deutschen Fußball ein Delikt aufklären sollte: 2012 warfen Anhänger des 1. FC Köln einen Pflasterstein auf einen Fanbus Mönchenbladbachs. Die DNA-Untersuchung des Wurfgeschosses führte zu keinem gerichtlich verwertbaren Ergebnis.

In Oberhausen erhielten 15 Extremfans im Frühjahr 2016 von der Stadt die Aufforderung, sich einer Medizinisch-Psychologischen Untersuchung (MPU), also dem sog. Idiotentest, zu unterziehen. Aufgrund ihres hohen Aggressionspotenzials sei davon auszugehen, dass die Ultras auch im Straßenverkehr impulsiv handelten: „Diverse polizeiliche Ermittlungen gegen Sie sind anhängig und aufgrund der Gruppierung auch in Zukunft zu erwarten." Laut Aussage der Ultras sind 13 der insgesamt 15 Betroffenen niemals rechtlich belangt worden. Der Fußball-Club Rot-Weiß Oberhausen meinte, der eventuelle Verlust des Führerscheins sei „ein bisschen viel". Auffällige Ultras würden ohnehin strafrechtlich verfolgt und bekämen Stadionverbot. Oktober wurden dann 4 Ultras per Verwaltungsakt angeschrieben, die MPU zu absolvieren. Da ihr Arbeitsplatz vom Führerschein abhängig ist, wollten sie der Aufforderung nachkommen.

André Schulz, Vorsitzender des Bundes Deutscher Kriminalbeamter (BDK), plädierte für mehr gegenseitiges Verständnis. Aggressivität sei kein Problem des Fußballs, besonders zunehmende Übergriffe auf „Amtspersonen des öffentlichen Dienstes" beträfen die gesamte Gesellschaft. Da mache der Fußball keine Ausnahme. „Ähnliches erleben wir leider auch zunehmend bei anderen Routineeinsätzen, etwa bei Verkehrskontrollen" (Ludwig/Poppe/Ruf, Heimliche Aufrüstung, Der Spiegel 46/2016, 108 ff.).

Baden-Württemberg

Stefan Brink wird neuer Datenschutzbeauftragter

Am 01.12.2016 wählte der Landtag von Baden-Württemberg mit 108 von 125 Stimmen den 49 Jahre alten Juristen Stefan Brink zum Landesbeauftragten für den Datenschutz (LfD) des Landes Baden-Württemberg. Er ist Nachfolger des bereits am 30.04.2016 aus dem Amt geschiedenen Jörg Klingbeil. Die lange Vakanz wurde zuvor kritisch gesehen, die späte Nachbesetzung erschien der heutigen Bedeutung des Datenschutzes unangemessen. Die lange Vakanz begründeten die Grünen wie folgt: Die alte grün-rote Landesregierung habe ihren Nachfolgern nicht vorgreifen wollen. Zum anderen bedürfe die sorgfältige Suche nach einem unabhängigen und qualifizierten Kandidaten eben Zeit.

Die Grünen hatten in der Landesregierung für den Posten das Vorschlagsrecht. Am 22.11.2016 bestätigte das Kabinett die Personalie. Der Vorsitzender der Grünen-Fraktion Andreas Schwarz erklärte, der Kandidat sei parteipolitisch unabhängig. Seine Fachlichkeit stehe „außer Zweifel".

Brink promovierte bei Prof. Hans Herbert von Arnim an der Deutschen Universität für Verwaltungswissenschaften in Speyer. Er war beim Wissenschaftlichen Dienst des Landtags Rheinland-Pfalz und später als Richter am Verwaltungsgericht Koblenz sowie als Wissenschaftlicher Mitarbeiter beim Bundesverfassungsgericht (1. Senat, Prof. Dr. Reinhard Gaier) tätig. Diesen Tätigkeiten folgte bis zu seinem Wechsel nach Baden-Württemberg seine Amtszeit als Leiter Privater Datenschutz beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit in Rheinland-Pfalz sowie als Stellvertretender Landesbeauftragter für die Informationsfreiheit Rheinland-Pfalz. Er ist Mitherausgeber eines Datenschutz-Standardkommentars.

Als Lehrbeauftragter ist Brink sowohl an der Deutschen Universität für Verwaltungswissenschaften Speyer als auch an der Europa-Universität Viadrina in Frankfurt/Oder engagiert (Landtag wählt Stefan Brink, http://www.stuttgarter-zeitung.de 01.12.2016; https://de.wikipedia.org/wiki/Stefan_Brink; Allgöwer, Stuttgarter Nachrichten 12.11.2016, 5; Ballarin, Aalens ehemaliger Vize-Polizeichef wird Bürgerbeauftragter, Aalener Nachrichten 12.11.2016, 2).

Berlin

Telefonica Next soll Datengeschäft in Schwung bringen

Telefonica Deutschland will mit einem konzerneigenen Datenanalyse-Startup dem Umsatzschwund im angestammten Mobilfunkgeschäft entgegentreten. Gemäß Firmenchef Thorsten Dirks ist hierfür in Berlin die Tochter Telefonica Next mit 50 MitarbeiterInnen gegründet worden: „Daten sind der Rohstoff der Zukunft.“ Das unter der Marke „o2“ bekannte Unternehmen will etwa in den Daten seiner 44 Mio. MobilfunkkundInnen nach Mustern suchen, die für andere Firmen wertvoll seien. So könnten Supermärkte etwa herausfinden, wann welche Waren gekauft werden. Dirks versprach, dass alle Datenschutzregeln streng eingehalten und die Angaben anonymisiert würden. „Wir wollen keine Kundendaten verkaufen, sondern an der Analyse Geld verdienen.“

Zudem setzt Telefonica auf das Vernetzen von Maschinen mit Sensoren. Die daraus gewonnen Daten sollen dann Entwicklern bereitgestellt werden. Marktexperten trauen den Geschäftsfeldern hohe Wachstumsraten zu. Die Unternehmensberatung McKinsey rechnet damit, dass die Zahl der vernetzten Geräte in Deutschland in vier Jahren 183 Mio. erreicht. Voriges Jahr waren es noch 82 Mio. Zu den erwarteten Umsätzen der 100-prozentigen Tochter, die von 2017 an von Ex-Vodafone-Manager Nicolaus Gollwitzer geführt wird, wollte Dirks nichts sagen.

Telefonica gehört zum gleichnamigen Telekomriesen aus Spanien und stieg durch die Übernahme des Rivalen E-Plus nach Kunden zum Marktführer auf. Wegen des starken Wettbewerbs mit der Telekom und Vodafone sowie von Behörden verordneten Gebührensenkungen wird der Umsatz im Mobilfunk im laufenden Jahr die 5,5 Milliarden Euro aus dem Jahr 2015 nicht erreichen (Start-Up soll Datengeschäft ankurbeln, www.handelsblatt.com 09.11.2016).

Berlin

BlnBDI beanstandet AfD-Werbung

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI) Maja Smoltczyk rügte die Parteivize der „Alternative für Deutschland“ (AfD) Beatrix von Storch wegen der Nutzung von personenbezogenen Daten für Werbezwecke. Von Storch betreibt ein Geflecht von Vereinen und Internet-Plattformen und hat Nutzende ihrer Seite Civilpetition.de und Abgeordneten-Check.de nicht hinreichend darüber informiert, dass sie deren Daten auch für Werbezwecke wie Newsletter verwendet: „Eine vorausgefüllte Einwilligung erfüllt diese Anforderung nicht“. Die BlnBDI prüft zudem weitere Hinweise der Internetaktivistin Katharina Nocun, dass in Storchs Vereinsgeflecht persönliche Daten von Nutzenden versendet werden. Deren Behörde forderte Storch auf, die Datenschutzhinweise für mehrere ihrer Internetseiten nachzubessern: „Es darf keine Sonderrechte für abgeordnetennahe Vereine geben, auch nicht für die AfD“ (Der Spiegel 52/2016, 34).

Hessen

Verfassungsschutz speichert weiter Friedensaktivistin

Eine 70 Jahre alte Aktivistin aus der Friedensbewegung muss im Rechtsstreit um ihre jahrelange Beobachtung durch den hessischen Verfassungsschutz weiter auf eine Entscheidung warten. Das Wiesbadener Verwaltungsgericht verwies den Fall am 12.01.2017 zurück zum Verwaltungsgericht Kassel, wo bereits eine Klage der ehemaligen Lehrerin anhängig ist. Die Tochter des Widerstandskämpfers und Verfolgten des NS-Regimes, Peter Gingold, will erreichen, dass die jahrelange Datensammlung und Speicherung des Verfassungsschutzes über ihre Aktivitäten von Anfang an rechtswidrig war und dass die Beobachtung eingestellt wird. Das Verfahren in Wiesbaden war von einer juristischen Auseinandersetzung in Kassel abgetrennt worden. In dem Prozess geht es um die Einsicht und Löschung aller ihrer Daten beim hessischen Verfassungsschutz. Der Vorsitzende Richter begründete seine Entscheidung zur Zuständigkeit des Kasseler Verwaltungsgerichts mit rein formalen Gründen. Inhaltlich ließ er sich nicht ein. Silvia Gingold, die von rund 100 SympathisantInnen aus dem linken Spektrum im und vor dem Gerichtssaal unterstützt wurde, äußerte sich enttäuscht nach dem Verfahren: „Für mich ist das ein rausreden und weiterschieben“ (Beobachtung durch Verfassungsschutz: Keine Entscheidung, www.focus.de 12.01.2017)

Mecklenburg-Vorpommern

Heinz Müller neuer Datenschutzbeauftragter

Der Landtag von Mecklenburg-Vorpommern hat am 07.12.2016 den früheren SPD-Landtagsabgeordneten Heinz Müller zum neuen Landesdatenschutzbeauftragten gewählt. Müller erhielt 38 von 68 abgegebenen Stimmen. Erforderlich waren 36. Für seinen Konkurrenten Karsten Neumann, den die Linken nominiert hatten, votierten elf Abgeordnete. Nur 49 der in geheimer Wahl abgegebenen Stim-

men waren gültig. Müller, dem nach der Landtagswahl vom 04.09.2016 den Wiedereinzug ins Parlament verpasste, weil sein Wahlkreis vom AfD-Kandidaten gewonnen wurde, folgt als Landesdatenschützer auf Reinhard Dankert, der in den Ruhestand geht.

Schwerpunkte seiner Arbeit sieht Müller vor allem in der Vereinheitlichung des Datenschutzrechts mit der ab 2018 geltenden neuen EU-Datenschutzverordnung. Zudem müsse das Bewusstsein für den Datenschutz vor allem bei jungen Menschen gestärkt werden, hatte Müller vor seiner Wahl gesagt. Der Datenschutz sollte seiner Meinung nach auch Teil der Lehrerbildung sein.

Zuvor hatte sich die Deutsche Vereinigung für Datenschutz (DVD) erfolglos in einem offenen Brief an die Landtagspräsidentin und die Fraktionsvorsitzenden des Landtags von Mecklenburg-Vorpommern gewandt mit der Aufforderung, die geplante Wahl des Landesbeauftragten für Datenschutz und Informationsfreiheit zu verschieben, ein transparentes Verfahren für die Auswahl der Kandidaten zu praktizieren und den besten Kandidaten zu bestellen.

Im Folgenden wird dieser offene Brief dokumentiert:

„Vor wenigen Tagen wurde bekannt, dass geplant sei, Heinz Müller Anfang Dezember dieses Jahres zum Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern zu wählen.

Gemäß Presseberichten hat der 62 Jahre alte, seit 18 Jahren im Landtag sitzende und zuletzt langjährige Parlamentarische Geschäftsführer der SPD-Fraktion den Wiedereinzug in den Landtag bei der Wahl am 04.09.2016 verpasst. Mit dem Thema Datenschutz habe er sich bisher „nicht so sehr beschäftigt“. Die Opposition spreche insofern von einem „Versorgungsposten“.

Die Deutsche Vereinigung für Datenschutz e.V. (DVD) hat hinsichtlich dieser Planung sowohl fachliche wie auch rechtliche Bedenken. Es geht dabei der DVD in keiner Hinsicht konkret um die Person von Heinz Müller, der in Datenschutzkreisen bisher völlig unbekannt ist und deshalb nicht bewertet werden soll. Vielmehr befürchtet die DVD, dass aus nichtfachlichen Gründen und unter Verletzung der am 25.05.2016 in Kraft getretenen Europäischen Datenschutz-Grundverordnung (DSGVO) die Bestellung eines Leiters einer Datenschutzaufsichtsbehörde (in der Terminologie des DSGVO eines „Mitglieds“) erfolgen soll:

In Art. 53 Abs. 1 DSGVO heißt es: „Jedes Mitglied muss über die für die Erfüllung seiner Aufgaben und Ausübung seiner Befugnisse erforderliche Qualifikation, Erfahrung und Sachkunde im Bereich des Schutzes personenbezogener Daten verfügen.“

Hinsichtlich des Auswahlverfahren heißt es in Art. 53 Abs. 1 DSGVO, dass „jedes Mitglied ihrer Aufsichtsbehörden im Wege eines transparenten Verfahrens“ zu ernennen ist. Diese Vorgaben werden in Art. 54 Abs. 1 DSGVO bekräftigt, wobei in lit d vorgesehen ist, dass bei Notwendigkeit „eine zeitlich versetzte Ernennung zur Wahrung der Unabhängigkeit der Aufsichtsbehörde“ erfolgen kann. Daraus ist abzuleiten, dass spätestens zum 25.05.2018 materiell die personellen Anforderungen an das „Mitglied“ erfüllt sein müssen.

Gemäß Art. 99 Abs. 2 DSGVO gilt die Grundverordnung vom 25.05.2018 an. Weiter heißt es: „Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.“ Gemäß dem im Europarecht anerkannten Prinzip der „Vorwirkung“ bzw. des „Frustrationsverbots“ dürfen auf nationaler Ebene keine Entscheidungen getroffen werden, die dem Ziel gültigen Europarechts entgegenstehen oder sie ernstlich gefährden (EuGH, U v. 22. 11. 2005, C-144/04 – Mangold). Bei der DS-GVO handelt es sich um gültiges Europarecht. Verstößt heute die Bestellung des Landesbeauftragten für Datenschutz und Informationsfreiheit (LfDI MV) gegen Europarecht, so hätte dies zur Folge, dass dieser Verstoß auch nach direkter Anwendbarkeit des DSGVO am 25.05.2018 direkte Wirkung entfaltet.

Zweck der o. g. Regelungen zur Bestellung von Datenschutzbeauftragten ist es, deren Qualifikation, Legitimation und Unabhängigkeit sicherzustellen, was für die Wahrung des digitalen Grundrechtsschutzes gemäß der Rechtsprechung des Bundesverfassungsgerichts wie auch nach Art. 8 Abs. 3 der Europäischen Grundrechte-Charta geboten ist.

Die Auswahl des Kandidaten für die Bestellung zum LfDI MV erfolgte nach unserem Eindruck nicht in einem – wie europarechtlich gefordert – transparenten Verfahren. Hierfür bedürfte es einer Ausschreibung und der danach eröffneten Möglichkeit einer demokratischen Debatte über die zur Wahl stehenden Kandidaten.

Es ist für uns aber auch nicht erkennbar, dass der Kandidat die europarechtlich geforderte „für die Erfüllung seiner Aufgaben und Ausübung seiner Befugnisse erforderliche Qualifikation, Erfahrung und Sachkunde, insbesondere im Bereich des Schutzes personenbezogener Daten“ mitbringt.

Dies hätte zur Folge, dass die Bestellung des derzeitigen Kandidaten gegen Europarecht verstoßen würde. Dies hätte zudem die Folge, dass die Gewährleistung eines demokratisch umfassend legitimierten, kompetenten und unabhängigen Datenschutzes gefährdet wäre. Dies hätte nicht nur für den Datenschutz in Mecklenburg-Vorpommern, sondern in Deutschland und wegen der Einbindung in die europäischen Entscheidungsprozesse (Art. 63 DSGVO) in Europa negative Auswirkungen.

Die geplante Personalentscheidung ist für die DVD zudem auch deshalb nicht nachvollziehbar, weil anscheinend nicht erwogen wurde, den bisherigen, qualifizierten und erfahrenen Amtsinhaber erneut zu bestellen oder auch dessen Stellvertreter, der sich bundesweit für den Datenschutz in größtem Maße verdient gemacht hat und in hervorragender Weise qualifiziert ist.

Wir fordern Sie daher dringend auf, die für den Dezember 2016 geplante Wahl des Landesbeauftragten Mecklenburg-Vorpommern zu verschieben, ein transparentes Verfahren zu dessen Bestellung zu wählen und die qualifizierteste Person auszuwählen, so wie dies auch von Art. 33 Abs. 2 Grundgesetz gefordert wird“.

Offensichtlich in Reaktion auf den offenen Brief der DVD rechtfertigte SPD-Fraktionsvorsitzender Thomas Krüger die Auswahl: „Heinz Müller ist sehr gut geeignet für das wichtige Amt. Als anerkannter Experte im Bereich der Innen- und Kommunalpolitik ist Heinz Müller seit vielen Jahren mit Fragen des Datenschutzes und der Informationsfreiheit vertraut. Von 1998 bis 2016 war Müller ununterbrochen Mitglied des für Datenschutz und Informationsfreiheit zustän-

digen Landtagsinnenausschusses. Zudem verfügt er als langjähriger Parlamentarischer Geschäftsführer über herausragende Erfahrungen an der Schnittstelle zwischen Politik und Verwaltung. Das sind aus unserer Sicht sehr gute Vorrausetzungen für das Amt des Datenschutzbeauftragten“ (Ex-Abgeordneter Heinz Müller neuer Datenschutzbeauftragter, www.ostsee-zeitung.de 07.12.2016; SPD-Fraktion schlägt Heinz Müller als neuen Datenschutzbeauftragten des Landes vor, www.spd-fraktion-mv.de 05.12.2016; DVD, Offener Brief 17.11.2016 https://www.datenschutzverein.de/wp-content/uploads/2016/11/2016-11-DVD-Brief-LfDI-MV.pdf).

Datenschutznachrichten aus dem Ausland

Weltweit

Riesen-Datenklau gegen Yahoo

Nach eigenen Angaben des Unternehmens Yahoo vom 14.12.2016 sind mehr als eine Milliarde Nutzende des US-Internetanbieters Opfer eines bislang unbekannten Hackerangriffs im Jahr 2013 geworden. Die Hacker hätten, so Sicherheitschef Bob Lord, wahrscheinlich im August 2013 persönliche Daten von mehr als einer Milliarde Konten, was darauf hindeutet, dass es sich damit um das größte bekannt gewordene Datenleck bei einem E-Mail-Provider überhaupt handelt. Die Cyberattacke sei von einer „nicht autorisierten dritten Partei“ geführt worden. Den Angaben zufolge dürften Namen, E-Mail-Adressen, Telefonnummern, Geburtsdaten, Passwörter und in manchen Fällen Sicherheitsfragen und -antworten entwendet worden sein. In dem offenbar betroffenen System seien aber keine Konto- oder Kreditkarten gespeichert gewesen.

Yahoo informierte die Betroffenen und setzte die Passwörter zurück. Unverschlüsselte Sicherheitsfragen wurden deaktiviert. Das Unternehmen wies Nutzenden zudem an, ihre Passwörter zu ändern und ihre Sicherheitsfragen ungültig zu machen. Yahoo hatte die Passwörter zwar auf zweifache Weise verschlüsselt - über Codierung und mit einer Technik namens Hashing. Doch können Hacker inzwischen gesicherte Passwörter knacken, indem sie riesige Lexika mit ähnlich verschlüsselten Begriffen anlegen und sie mit Datenbanken gestohlener Passwörter abgleichen. Dadurch könnten UserInnen in Schwierigkeiten geraten, die ihr Yahoo-Passwort auch für andere Online-Konten nutzen. Yahoo geht davon aus, dass es sich bei dem nun bekannt gegebenen Hack um einen anderen Vorfall als den Hackerangriff von 2014 handele, bei dem rund 500 Millionen Konten betroffen waren. Diese Cyberattacke hatte Yahoo im September 2016 bekannt gemacht. Bei dem nun eingeräumten Hackerangriff ging um dem Unternehmen zufolge um dieselbe Art von Daten. Es ist unklar, wann Yahoo von dem Hack Kenntnis erlangt hat. Am 07.11.2016 hatten Sicherheitsbehörden der Firma gehackte Daten zur Kenntnis gegeben. Der Konzern vermutet, dass beide Attacken von denselben Angreifern im Auftrag eines Staates ausgingen. Welchem Land sie zugerechnet werden, ist bis heute nicht mitgeteilt worden. Der Sicherheitsanalyst Andrew Komarow erklärte, dass eine osteuropäische Hackergruppe die Daten angeboten habe.

Yahoo erklärte, man wisse noch nicht, wie die Angreifer in das System gekommen seien, was vom IT-Sicherheitsexperten Bruce Schneier kommentiert wurde: „Yahoo hat richtigen Mist gebaut. Man sieht jetzt, dass sie Sicherheit nicht ernst genommen haben“. US-amerikanische BürgerrechtlerInnen zweifeln ohnehin generell an der Vertrauenswürdigkeit des Unternehmens. Zwei ehemaligen Beschäftigten zufolge scannt das Unternehmen E-Mails für amerikanische Sicherheitsbehörden wie NSA und FBI nach bestimmten Schlagworten.

Der neuerliche umfangreiche Diebstahl von Kundendaten gefährdet die geplante Übernahme Yahoos durch den Telekommunikationsriesen Verizon mit einem Volumen von rund 4,8 Milliarden Dollar. Der Telekomkonzern kündigte dazu an, die Situation im Rahmen der Ermittlungen bei Yahoo im Blick zu behalten. Ehe eine endgültige Entscheidung getroffen werde, so Sprecher Bob Varettoni, würde die „neue Entwicklung“ geprüft. Yahoo zeigte sich zuversichtlich, dass die neueste Bekanntmachung den Verkauf an Verizon nicht bedroht. Yahoo sei während der Untersuchung in ständigem Kontakt mit Verizon gewesen (www.handelsblatt.com 14./15.12.2016, Yahoo meldet größten Datenklau aller Zeiten; Kuhn, „Richtig Mist gebaut“, SZ 16.12.2016, 15).

Weltweit

Facebook legt Patientenkontaktdaten offen

Eine Psychiaterin, die Facebook nutzt, konnte sich nicht erklären, warum sie sich gemäß dem Vorschlag des sog. sozialen Netzwerks plötzlich mit ihre PatientInnen befreunden sollte. Auch ihre PatientInnen berichteten ihr, dass sie andere, die sie etwa in der Praxis getroffen hatten, plötzlich auf Facebook fanden.

Für die Psychiaterin stellt dies ein großes Vertraulichkeits-Problem. Ihre Patienten-Daten müssen vertraulich behandelt werden. Alleine, dass andere die Namen ihrer MitpatientInnen herausfinden, könnte sogar zum Sicherheitsrisiko werden. Ihr erster Verdacht war, dass es damit zusammenhängt, dass sich alle Personen einmal am gleichen Ort aufgehalten hatten. Facebook hatte das jedoch zurückgewiesen und gemeint, dass keine Accounts nach ihrer Location empfohlen werden würden.

Daher besteht die Vermutung, dass die Empfehlungen auf die Angabe ihrer Telefonnummern auf Facebook durch die Psychiaterin und deren PatientInnen zurückgeht. Wenn Kontakte aus dem Adressbuch importiert werden, sind sie miteinander verknüpft. Im privaten Umfeld kann das Feature prak-

tisch sein, doch im beruflichen Kontext kann es, wie hier, zu großen Problem führen, zumal es keine Vorwarnung und keine Erklärung für die Nutzenden gibt, dass dies passieren wird. Ein Sprecher von Facebook bestätigte die Vermutung nicht, widerlegte sie aber auch nicht: „Die Auswahl von Freundschaftsvorschläge basiert auf vielfältigen Faktoren, einschließlich gemeinsamen Freunden, Berufs- oder Ausbildungsinformatioen, gemeinsam genutzten Netzwerken, importierten Kontakten und anderen Faktoren.“

Dies ist ein weiterer Grund, weshalb auch die Datenweitergabe der Whatsapp-Telefonnummern an Facebook kritisch zu sehen ist (Plötzlich wurden einer Psychiaterin ihre Patienten auf Facebook vorgeschlagen: Wie kann das sein? t3n.de 30.08.2016; Scotti, Facebook recommended that this psychiatrist´s patients friend each other, www.fusion.net 29.08.2016).

Europa

System für visumfreie Einreise in die EU geplant

Die Europäische Union (EU) will ein Verfahren einführen, mit dem DrittausländerInnen sich vor einer visumfreien Einreise in den EU-Raum elektronisch anmelden müssen. Die EU-Kommission will damit eine Sicherheitslücke schließen. Sie präsentierte am 16.11.2016 ihren Vorschlag für ein europäisches Reise-Informations- und Genehmigungssystem (Etias). Vizepräsident Frans Timmermans begründete die Initiative: „Wir können dann wissen, wer unsere Grenze überschreitet. Das wissen wir bisher nur bei Inhabern von Visa.“ Betroffen sein sollen also BürgerInnen aus Nicht-EU-Staaten, die für eine Reise nach Europa kein Visum benötigen, sondern nur einen Reisepass, also z. B. Menschen aus den USA, Japan, Taiwan, Malaysia, Serbien oder Mazedonien. Die Liste umfasst knapp 60 Länder, nach dem Brexit dürfte wohl auch Großbritannien dazu kommen.

Vorbild für die Initiative ist das US-amerikanische Esta-Verfahren. So benötigen z. B. EU-BürgerInnen für eine Reise in die USA zwar kein Visum, wohl aber seit 2009 eine Reisegenehmigung. Sie ist vor Fahrtantritt online zu beantragen und kostet 14 Dollar. Verlangt werden diverse persönliche Angaben, unter anderem über Schulbildung, Job, Vorstrafen und Krankheiten. Gibt das Esta-System grünes Licht, garantiert dies zwar noch keine Einreise in die USA, verkürzt aber die Überprüfung an der Grenze, die nach den Anschlägen von 9/11 stark verschärft worden war.

Gemäß Timmermann ist das geplante System „billig, leicht und effizient“. Alles geschehe gemäß den neuesten Datenschutzregeln der EU, die in Brüssel als „die besten der Welt“ gelten. Das Ausfüllen dauere nur wenige Minuten und werde in 95 Prozent aller Fälle wiederum in Minuten zu einer positiven Antwort führen. Die Daten werden automatisiert mit den einschlägigen europäischen Datenbanken abgeglichen. Dazu zählen das Schengener Informationssystem, die Asylbewerber-Datenbank Eurodac, das Visa-Informationssystem oder die Datenbanken von Europol und Interpol. Hinzukommen wird das geplante Ein- und Austrittssystem der EU, mit dem künftig jene ermittelt werden sollen, die sich länger im Schengen-Gebiet aufhalten, als sie dürfen. All dies soll miteinander zu einer IT-Architektur verbunden werden, die langfristig eine einfache, einheitliche Benutzer-Oberfläche erhalten soll.

In Kommissionskreisen wurde gesagt, Etias wolle von Reisenden im Vergleich zu den Systemen in den USA, Kanada oder Australien nur „das absolute Minimum“ erfahren. Gefragt wird nach Personal- und Adressdaten, ansteckenden Krankheiten, Vorstrafen, Aufenthalten in Kriegs- oder anderen Risikogebieten, Ausweisungen aus der EU, aber auch nach Ausbildung und Jobsituation. Schlägt das System an, sollen EU-Mitarbeitende oder nationale Behörden der Sache nachgehen. Diverse Sonderfälle, wie etwa GrenzgängerInnen, würden berücksichtigt, versichert die Kommission; Internet-Ferne oder Analphabeten können Vertreter mit der Anfrage beauftragen.

Der Aufbau von Etias soll einmalig 212 Millionen Euro kosten. Die jährlichen Kosten von 85 Millionen sollen von den fünf Euro Gebühren gedeckt werden, die zwischen 30 bis 50 Millionen Reisende im Jahr pro Etias-Überprüfung bezahlen müssen. Eine Genehmigung soll fünf Jahre lang gültig sein. Geplant ist, das System in drei Jahren in Betrieb zu nehmen.

Die Grünen im EU-Parlament halten das System für unnötig. Es koste, so der Abgeordnete Jan Albrecht, zu viel und werde wenig Mehrwert bringen. Schließlich seien Bürger aus Staaten betroffen, die ohnehin diverse rechtsstaatliche Bedingungen der EU erfüllen müssten und mit denen die EU schon polizeilich und justiziell zusammenarbeite. Ein solches System wiege die BürgerInnen nur in „Schein-Sicherheit“ und könne sogar weniger Sicherheit bedeuten, weil dafür Kapazitäten bei der Ermittlung abgezogen würden. Monika Hohlmeier (CSU) widersprach. Etias liefere den EU-Grenzbeamten wertvolle Informationen. So könne man nicht zuletzt Schwerverbrechern und Mitgliedern krimineller Netzwerke auf die Schliche kommen, die immer raffiniertere Täuschungsmittel ersönnen und sich oftmals frei auf europäischem Gebiet bewegen könnten: „Damit sind wir bisher zu locker umgegangen“ (Kirchner, Europa will´s wissen, SZ 17.11.2016, 8).

Frankreich

Innenminister schafft per Dekret Bevölkerungsdatenbank

Der französische Innenminister Bernard Cazeneuve baut per Dekret, also ohne ausdrückliche Gesetzesgrundlage, eine neue Datenbank auf, in der die Angaben der mehr als 60 Millionen BürgerInnen zentral gespeichert werden, und zwar nicht nur Name, Geburtsdatum und Adressen, sondern auch biometrische Daten wie Fingerabdrücke aus Pässen und Ausweisen. Die Sicherheitsbehörden auf diese Daten online Zugriff nehmen können. per Knopfdruck abrufbar sein. MenschenrechtlerInnen, DatenschützerInnen wie auch sozialistische Parteifreunde warnen vor Staatskontrolle und werfen Cazeneuve vor, er zeuge „eine Art Monster“. Nach tagelangen Protesten kündigte dieser zwar Mitte November 2016 zwar einige Konzessionen an. So sollen seine Citoyens (Bürger) das Recht erhalten, bei der Beantragung ihrer nächsten „Carte d‘Identité“, des Personalausweises, der

Speicherung ihrer biometrischen Daten zu widersprechen. Zudem konzedierte der Minister, Nationalversammlung sowie Senat sollten über seine Mega-Datenbank im Parlament beraten dürfen. Das ändert aber nichts daran, dass Cazeneuves Dekret in Kraft bleibt.

Der leise und meist unauffällig agierende Innenminister rechtfertigt die Datenbank als Mittel im Kampf gegen organisierte Kriminalität und Terrorismus. Das Dekret wurde im Laufe des Ferienwochenendes vor Allerheiligen im Amtsblatt veröffentlicht, was Argwohn sogar innerhalb des Kabinetts schürte: Cazeneuves Kollegin Axelle Lemaire, für Datenschutz zuständige Staatsministerin, fühlte sich hintergangen und sprach von einer „klammheimlichen Entscheidung". Lemaire lenkte inzwischen ein, auch weil das Innenministerium zusagte, das Zentralregister namens TES (Titres Electroniques Sécurisés) werde von unabhängigen ExpertInnen überprüft, ob es hinreichend gegen Hackerangriffe geschützt sei. Seit dem 08.11.2016 ist TES probeweise in Betrieb.

Die Sorge vor Missbrauch ist äußerst gegenwärtig. Selbst Frankreichs Datenschutzbehörde, die Commission Nationale de l´Informatique et des Libertés (CNIL), befürchtet Missbrauch seitens des Staats. Zwar beteuert Minister Cazeneuve, die Datenbank diene dazu, bei Kontrollen die Angaben von BürgerInnen zu beglaubigen. Die weiter reichende Identitätsermittlung eines Unbekannten, etwa per Abgleich von Fingerabdrücken, sei untersagt. Dies beruhigte die CNIL nicht. Die französische Regierung hatte schon bei anderen Datenbanken nachträglich die Nutzungsmöglichkeiten durch Polizei oder Geheimdienst erweitert. Zudem sei die Gefahr des Missbrauchs der Datenbank durch eine andere, autoritäre Regierung heute größer denn je: „Demokratische Rückschläge sowie das Anwachsen des Populismus, wie wir ihn in Europa und den Vereinigten Staaten beobachten, machen dies zu einer wahnwitzigen Wette auf die Zukunft." Die CNIL hatte offenbar Marine Le Pen vor Augen, die Vorsitzende von Frankreichs Front National. Donald Trump war bei Verfertigung des Gutachtens noch nicht gewählt. Inzwischen kündigten einzelne BürgerInnen sowie die Liga für Menschenrechte an, gegen Cazeneuves Daten-Dekret vor dem Staatsrat zu klagen (Wernicke, Angst vor dem Daten-Monster, SZ 12./13.11.2016, 8).

Belgien

Identifikationspflicht bei europainternen Reisen

Aus Angst vor neuen Terroranschlägen will die belgische Regierung ab 2018 Reisende auch innerhalb der EU strenger kontrollieren. Danach müssen sich nicht nur Flugpassagiere registrieren lassen, sondern auch alle Personen, die mit Bus, Bahn oder Schiff ins europäische Ausland fahren. Nach Ansicht des belgischen Innenministers Jan Jambon hat die Flucht des mutmaßlichen Terrorattentäters auf dem Weihnachtsmarkt in Berlin gezeigt, dass ein Tatverdächtiger offenbar ohne Probleme mehrere Grenzen passieren konnte. Der Berlin-Attentäter war mit Regionalzügen unterwegs, weil man z. B. in französischen Schnellzügen schon heute namentlich gekennzeichnete Platzkarten benötigt. Angesichts dieser Tatsache, so der Minister, könnten nun auch andere Länder vom Nutzen einer EU-weiten Passagierdaten-Erfassung bei international verkehrenden Zügen, Bussen und Booten überzeugt werden.

In Belgien hat die Abgeordnetenkammer kurz vor Weihnachten ein entsprechendes Gesetz gebilligt. Demnach soll die vom EU-Parlament 2016 beschlossene Speicherung von Fluggastdaten von Mai 2018 an auch für andere Verkehrsmittel gelten. Bahn-, Bus- und Fährgesellschaften, die ihrer Meldepflicht nicht nachkommen, riskieren eine Geldbuße von bis zu 50 000 Euro pro nicht erfolgter Registrierung. Für die KundInnen hat dies voraussichtlich längere Wartezeiten zur Folge. Auch die Möglichkeit, kurz vor Abfahrt in einen Zug zu springen, wird es dann wohl nicht mehr geben. Die Passagiere müssten sich beim Kauf der Fahrkarte ausweisen.

Die EU-Kommission erörterte die praktischen Auswirkungen mit der belgischen Regierung. Sie gab das Signal, dass sie nichts dagegen hat, so ein Kommissionssprecher: „Die Mitgliedsstaaten können ein System für die Erhebung und Verarbeitung von Passagierdaten auch für andere Verkehrsträger als den Luftverkehr vorsehen, wenn das nationale Recht dem EU-Recht entspricht." Der für Sicherheitsfragen zuständige EU-Kommissar Julian King erklärte anlässlich des Dreikönig-Klausurtreffens der CSU-Landesgruppe im Kloster Seeon: „Das ist ein legitimes Anliegen." Die belgische Regierung hat angekündigt, vor dem tatsächlichen Inkrafttreten des Gesetzes mit den Nachbarstaaten zu sprechen, so Jambon: „Wir befinden uns in Gesprächen mit Niederlanden, Frankreich und Deutschland". Es sei wichtig, dass sich möglichst viele Länder beteiligen. Belgien versteht sich, auch wegen der Terroranschläge von Brüssel im März 2016, als Vorreiter in Sicherheitsfragen. Ein Sprecher des Innenministeriums meinte: „Terroristen wählen den Weg des geringsten Widerstands."

Der europäische Bahnverband CER hat in einem Protestbrief an den belgischen Premierminister Charles Michel vor negativen Konsequenzen gewarnt. Es seien gerade die Flexibilität und der offene Zugang, die das Bahnfahren attraktiv machten. Datenerhebung und Kontrolle seien derart aufwändig, dass dadurch Menschen vergrätzt und zum Ausweichen auf das Auto veranlasst würden. Gemäß CER läuft die Maßnahme dem Schengener Abkommen über grenzkontrollfreies Reisen in Europa zuwider. Auch die Deutsche Bahn kritisiert, das Vorhaben habe „weitreichende Auswirkungen auf den Eisenbahnverkehr zwischen Deutschland und Belgien und könnte die Freizügigkeit unserer Kunden in Frage stellen" (Mühlauer, Belgien verschärft Kontrollen für Reisen, Steinke, Viele kleine Niederlagen, SZ 03.01.2016, 1, 4; Belgien darf Züge kontrollieren, Der Spiegel 2/2017, 20).

Niederlande

360-Grad-Handgepäckscanner für Flughafenkontrollen

Am Flughafen von Amsterdam Schiphol wird ein neuer Gepäck-Scanner getestet, bei dem es nicht mehr nötig sein soll, den Laptop und die Creme aus dem Handgepäck herauszuholen. Er ermöglicht es dem Sicherheitspersonal, den Inhalt der Taschen oder Rucksäcke auf dem

Bildschirm in einer 360-Grad-Umsicht zu inspizieren. Für die Reisenden soll sich der Vorteil ergeben, dass möglicherweise problematische Stücke nicht mehr ausgepackt werden müssen. Bisher sollen nach Fachmedienberichten zwei solcher Stationen in Betrieb sein. Die Vorschrift, Cremes, Zahnpasta und Ähnliches in einer Plastiktüte von maximal 100 Milliliter verstauen zu müssen, bleibt vorläufig bestehen. Der Test soll bis Ende 2017 laufen (Neue Scanner im Test, SZ 17.11.2016, 39).

Großbritannien

Investigatory Powers Bill in Kraft

Nach Zustimmung der Queen ist mit dem Investigatory Powers Bill (bzw. Act – IPB bzw. IPA) in Großbritannien eines der weltweit weitestgehenden Überwachungsgesetze in Kraft getreten. Es verpflichtet unter anderem Internetanbieter dazu, für jede KundIn eine Liste aller besuchten Internetseiten zwölf Monate lang zu speichern. Nach richterlicher Anordnung müssen selbst die Listen kontaktierter Telefonnummern und aufgerufener Internetseiten von JournalistInnen ausgehändigt werden. Das Gesetz gibt Sicherheitsbehörden die Erlaubnis, selbst zu Hackern zu werden und massenhaft Überwachungsdaten zu sammeln. Nachdem eine Petition gegen das Gesetz genügend Unterzeichnende gefunden hat, muss sich aber das Parlament noch einmal damit befassen.

Kommunikationsanbieter müssen künftig technische Schutzmaßnahmen beseitigen, um Behörden den Zugriff auf Inhalt zu ermöglichen. Dies kann in der Form erfolgen, dass Entwickler künftig Hintertüren oder Schwachstellen in eigene Produkte einbauen, über die ihre KundInnen überwacht werden können. Einige nach anfänglicher Kritik eingeflossene Änderungen haben die damit verbundenen Eingriffsmöglichkeiten nicht entscheidend abgeschwächt.

Die britische Innenministerin Amber Rudd lobte das Gesetz nach seinem Inkrafttreten als „weltweit führende Gesetzgebung“, die „bislang unerreichte Transparenz“ mit „grundlegendem Datenschutz“ verbinde. Dem widersprechen Datenschützer vehement. So nennt die Open Rights Group den IPA als eines der extremsten Überwachungsgesetze, die jemals in einer Demokratie verabschiedet wurden. Seine Auswirkungen würden weltweit zu spüren sein, wenn sich autoritäre Regime dadurch zu ähnlichen Maßnahmen ermuntert fühlen (Holland, Großbritannien: Massives Überwachungsgesetz inkraft getreten, www.heise.de 30.11.2016; vgl. DANA 1/2016, 30 f., DANA 3/2016,146).

Großbritannien

Test mit Identifizierungspflicht bei Wahlen

Die britische Regierung plant die Einführung einer formellen Identifizierung bei Wahlen. Bisher mussten die WählerInnen im Wahllokal weder Ausweis noch Wahlkarte vorlegen. Es genügte, den Namen anzugeben, der im Wählerregister verzeichnet war – idealerweise den eigenen. Es war bisher jederzeit möglich, einen anderen anzugeben. Da dieses System vereinzelt zu Missbrauch geführt hat, soll es geändert werden. Die britische Regierung erklärte am 27.12.2016, zunächst solle in 18 Wahlbezirken getestet werden, wie sich die Pflicht zur Identifizierung in der Praxis umsetzen lässt. Bei den Kommunalwahlen im Mai 2018 werden in ausgewählten Bezirken verschiedene Methoden getestet. In manchen Wahllokalen soll der Reisepass vorgelegt werden müssen, in manchen der Führerschein oder die Kreditkarte, in anderen soll der Nachweis über offizielle Korrespondenz wie Strom- oder Gasrechnungen erfolgen. Erweisen sich die Tests als Erfolg, soll die Pflicht zur Identifikation landesweit eingeführt werden.

Hintergrund der Problematik bei der Wähleridentifikation ist, dass, anders als z. B. in Deutschland, in Großbritannien keine Ausweispflicht besteht. Viele Briten verfügen über keinen Pass und überhaupt über keinerlei offizielles Ausweisdokument. Die Labour-Regierung hatte 2008 nach jahrelangen Diskussionen eine Art Personalausweis eingeführt, den die Konservativen nach ihrem Wahlsieg gleich wieder abschafften (vgl. DANA 2/2008, 82; 3/2019, 116; 4/2010, 158 f.). Je nachdem, welche Form von Identitätsnachweis eingeführt wird, könnten daher BürgerInnen künftig von den Wahlen ausgeschlossen sein. Menschen ohne Pass und Führerschein gehören i. d. R. zu den ärmeren und bildungsfernen Schichten, also jenen, die sich ohnehin von der Politik abgehängt fühlen (Zaschke, Ausweis bitte, London testet Ausweispflicht, SZ 28.12.2016, 4, 11).

Großbritannien

Facebook gegen Datennutzung durch Versicherung

Der britische Versicherer Admiral wollte im Gegenzug für günstigere KfZ-Tarife die Facebook-Profile seiner KundInnen auswerten. Da junge AutofahrerInnen in der Regel höhere Versicherungsbeiträge zu zahlen haben, hatte sich Admiral zur Risikobewertung Folgendes überlegt: Die jungen Menschen erhalten unter der Überschrift „Firstcarquote“ Vergünstigungen, wenn sie sich bereit erklären, dass ihr Facebook-Profil durchleuchtet wird. Das Unternehmen erklärt, daraus ließen sich nicht nur Rückschlüsse auf dessen Kreditwürdigkeit ziehen, sondern auch auf dessen Fahrverhalten: „Unsere clevere Technologie erlaubt es uns vorherzusagen, wer wahrscheinlich ein sicherer Fahrer ist“, heißt es weiter in der Mitteilung.

Admiral wollte die Facebook-Profile der KundInnen dahingehend untersuchen, ob diese gewissenhaft und gut organisiert erscheinen. Hinweise hierauf sollen sein, wenn die User kurze, konkrete Formulierungen verwendeten und beispielsweise bei Terminvereinbarungen konkrete Angaben zu Ort und Zeit machten, anstatt einfach nur „heute Abend“ zu sagen. Den KundInnen, die sich hierzu bereit erklären, sollten Preisnachlässe bis zu 15% gewährt werden. Noch größer würde der Rabatt ausfallen, wenn sich die jeweiligen KundInnen zur Installation einer Blackbox in ihr Auto bereit erklären würden.

Gemäß Pressemeldungen hat Facebook diesen Plänen einen Riegel vorgeschoben. Zwar dürfe der Versicherer die Facebook-Accounts zur Kundenverifikation verwenden, nicht jedoch, die Accounts der Facebook-User auszuwerten,

um hieraus Rabatte zu errechnen. Ein Facebook-Sprecher begründete dies mit Verweis auf Datenschutzbestimmungen (Thaler, Datenschutz: Facebook schiebt Versicherer-Plänen Riegel vor, www.procontra-online.de 02.11.2016).

USA-Europa

Trump verunsichert Datenschützer

Datenschutz ist zwischen den USA und der EU schon traditionell ein mühsames Geschäft. Jetzt wächst die Unsicherheit, was die Trump-Regierung will. Der am 20.01.2017 ins Amt eingeführte US-Präsident Donald Trump hat es mit einem seiner Erlasse, einer „Executive Order" zur Verschärfung der Einwanderungspolitik, auch sein erstes offizielles Statement zum Datenschutz abgegeben. Er hat die Behörden in den USA, für die der Privacy Act gilt, aufgefordert, den Datenschutz für Nicht-US-Bürger aufzuheben, „soweit das mit dem Gesetz vereinbar ist". Unklar ist nun, ob auch das Klagerecht von EU-Bürgern nach dem Juridical Redress Act", der erst im Februar 2017 in Kraft tritt, zurückgenommen werden soll. Unklar ist auch, inwieweit die Datenschutzvereinbarung des EU-U.S.-Privacy Shield von dieser Einschränkung betroffen ist, die ja keine Gesetzeskraft hat. Eine Regelung des Datenschutzes ist für den Austausch von Daten in privaten Unternehmen über den Atlantik sehr wichtig. Sie war nötig geworden, weil der Europäische Gerichtshof 2015 eine Neuregelung des löchrigen Datenschutzes verlangt hatte. Betroffen ist auch der Zugriff amerikanischer Geheimdienste und Ermittlungsbehörden auf diese Daten. Das Privacy Shield ist kein richtiger Vertrag, sondern nur eine Verabredung zwischen der alten US-Regierung und der EU-Kommission in Brüssel. Rund 1.500 US-Unternehmen nutzten Ende Januar 2017 die Datenschutzvereinbarung für ihre europäischen Geschäfte. Würde es die Regelung nicht geben, dürften zum Beispiel Facebook, Google, Amazon und andere die Daten europäischer KundInnen nur noch auf geschützten Servern in Europa verarbeiten und auch nur hier verkaufen.

Der Datenschutz-Experte des Europäischen Parlaments, der grüne Abgeordnete Jan Philipp Albrecht, hat – mit dem Medium Trumps, also Twitter – reagiert: „Wenn das zutrifft, dann muss die EU-Kommission ‚Privacy Shield' sofort aussetzen und die USA bestrafen." Nach US-Presseberichten soll sich der Erlass des Präsidenten nicht auf den Datenschutz für EU-BürgerInnen beziehen. Der sei eher als Warnung an Einwanderer aus Nicht-EU-Staaten gemeint gewesen. Die für den Datenschutz und damit auch das Privacy Shield hauptverantwortliche EU-Justizkommissarin Vera Jourova meinte: „Wir fragen uns alle, was da in den USA vorgeht. Auf jeden Fall werden wir unsere Datenschutz-Standards nicht absenken. Das ganze Abkommen mit den USA basiert auf Vertrauen – Vertrauen in die amerikanische Regierung. Und dieses Vertrauen muss erst einmal erneuert oder hergestellt werden.". Zu diesem Zweck hat sie einen Brief an die US-Regierung gesendet und um Klarstellung gebeten. Die Kommissarin will März/April 2017 nach Washington reisen, um sich mit ihren neuen Verhandlungspartnern in der Trump-Administration, dem designierten Handelsbeauftragten Wilbur Ross und möglichst auch mit dem neuen Justizminister, zu treffen. Sie hoffe, so Jourova, auf gute Gespräche in Washington, werde aber „sehr strikt" sein, wenn es um Datenschutz gehe.

Laut US-Presseberichten will Trump auch, dass Einreisende in die USA ihre Social-Media-Profile, Telefonkontakte und Websites offenlegen. AusländerInnen, die sich weigern, ihre Informationen zu teilen, solle nach dem Wunsch Trumps die Einreise verweigert werden können. Dieses Vorhaben habe bislang aber erst eine niedrige Diskussionsebene. Grund für diesen Plan sei der San-Bernadinho-Terrorist Tashfeen Malik, der unter einem Pseudonym und erhöhter Privatsphäre in sozialen Medien vor seinem Anschlag den Jihad gefordert hat. Ende 2016 wurde bereits eine ähnliche umstrittene Änderung in der Informationsabfrage bei Touristen umgesetzt. Personen, die im Rahmen des Visa-Waiver-Programms einreisen, finden im dafür notwendigen ESTA-Antrag ein Drop-Down-Menü, das nach deren Social-Media-Profilen fragt. Die Eingabe ist allerdings bisher optional. Unter Trump könnte sich diese Regel verschärfen. Der Regierungssprecher Sean Spicer gab auf CNN-Anfrage keinen Kommentar zu dem aktuellen Bericht.

Die Maßnahme dient gemäß einem Sprecher dazu, dass „potenzielle Gefahren identifiziert" werden. Access Now, eine Non-Profit-Organisation für Menschenrechte im digitalen Zeitalter, befürchtet aber, dass sich TouristInnen schon jetzt eingeschüchtert fühlen und die Accounts zur Sicherheit angeben. Datenschützer hatten schon im Juli 2016 befürchtet, dass auch andere Länder ähnliche Einreisebestimmungen umsetzen werden (Riegert, EU rätselt: Attackiert Trump den Datenschutz?, http://www.dw.com/de 27.01.2017; Trump will, dass Einreisende ihre Social-Media-Profile, Telefonkontakte und Websites offenlegen, t3n.de 30.01.2017; Oberndorfer, Social-Media-Accounts beim ESTA-Antrag, t3n.de 23.01.2017).

USA

Berufungsgericht: Kein Behördenzugriff auf in Irland gespeicherte Daten

Ein Bundesberufungsgericht der Vereinigten Staaten (United States Court of Appeals for the Second Circuit) hat am 24.01.2017 entschieden, den Fall Microsoft gegen die US-Regierung nicht erneut aufzurollen, so dass sein Urteil vom 14.07.2016, nach dem Microsoft im Ausland gespeicherte Kommunikationsinhalte von Kunden nicht an Strafverfolger ausliefern muss, weiterhin Bestand hat.

In dem langjährigen Rechtsstreit geht es ursprünglich um eine Aufforderung von US-Behörden an Microsoft aus dem Jahr 2013, ihnen E-Mails eines mutmaßlichen Drogenschmugglers auszuhändigen. Microsoft stellte nur die in den USA gespeicherten Account-Daten zur Verfügung und weigerte sich, die in Irland gespeicherten E-Mails herauszugeben, da der von einem New Yorker Bezirksrichter unterschriebene Durchsuchungsbefehl im Ausland nicht gültig sei. Die Regierung hatte argumentiert, Microsoft habe Zugriff auf die Inhal-

te; deshalb seien diese als in den USA verblieben zu betrachten. Ein Bundesgericht gab zunächst der US-Regierung Recht, doch wurde dieses Urteil im Juli 2016 aufgehoben.

Die Entscheidung war damals durchaus knapp, ein Richter der zuständigen Kammer votierte für die Sichtweise der US-Regierung, zwei für den von der Electronic Frontier Foundation unterstützten IT-Riesen. Das US-Justizministerium hatte daraufhin beantragt, dass der Fall nochmal in einer sogenannten „en banc"-Session von allen Richtern des zweiten Bezirks des Berufungsgerichts geprüft wird. Dieser Antrag ist aufgrund eines Patts unter den Richtern jetzt gescheitert: Vier von ihnen stimmten für den Antrag und vier dagegen. Es ist zu vermuten, dass das Justizministerium nun vor den Obersten Gerichtshof zieht.

Wie lange der als Erfolg für den Datenschutz gefeierte Sieg des Technologie-Konzerns bestand hat, ist fraglich. Die Entscheidung des Gerichts beruhte nicht auf grundsätzlichen Bedenken in Hinblick auf den Schutz der Privatsphäre, sondern lediglich auf formalen Bedenken. Die Richter stellten fest, dass negative Konsequenzen der Entscheidung für die nationale Sicherheit Gesetzesverschärfungen nach sich ziehen könnten (Dachwitz, US-Gericht: Microsoft muss im Ausland gespeicherte Mails weiterhin nicht an Strafverfolger liefern, netzpolitik.org 25.01.2017; Sieg für Microsoft, SZ 26.01.2017, 21).

Technik-Nachrichten

Software manipuliert Sprachaufnahmen

Eine neue Software von Adobe ist in der Lage, Sprachaufnahmen so verändern, dass ein Mensch etwas völlig anderes zu sagen scheint als im Original. Damit ergeben sich völlig neue Möglichkeiten für Fälschungen, Verzerrungen, Lügen und Manipulationen in Tondokumenten. Adobe präsentierte in San Diego/USA das Programm, mit dem in der Stimme einer beliebigen Person Worte und ganze Sätze geformt werden können. Das Projekt mit dem Titel „VoCo" ist bisher noch nicht auf dem Markt frei verfügbar. Mit der Software könnten Tonaufnahmen massenhaft gefälscht, verändert, umgeschrieben werden, so wie dies heute bereits bei Bildern der Fall ist. Nahezu alle Fotos, die ein Mensch im öffentlichen Raum sieht, sind heute bereits bearbeitet, die meisten davon übrigens mit einem anderen Produkt von Adobe, der weit verbreiteten Software Photoshop.

Bei der Software-Präsentation veränderte ein Adobe-Manager auf der Bühne aufgezeichnete Sätze, die ein Komiker nur Minuten vorher auf der Bühne ausgesprochen hatte. Zunächst verschob der Manager lediglich Worte innerhalb der aufgenommenen Sätze des Komikers. Das ist mithilfe von Schnittprogrammen seit Jahren möglich. Dann aber fügte der Adobe-Manager ganz neue Worte, die er in eine Tatstatur schrieb, in den Satz des Komikers ein. Die Software gab die Worte in der Stimme des Komikers über einen Lautsprecher aus und vermittelte über den Rhythmus des gesamten Satzes den Eindruck normaler Sprache. Die Software benötigt dazu nach Angaben von Adobe lediglich etwa 20 Minuten Tonbandaufnahme von der Person, deren Worte sie imitieren soll, sowie ein Transkript des Gesprochenen. Sie zerlegt die Worte in einzelne Laute, aus denen sie wiederum neue Wörter zusammenbauen kann. Die Computer-Stimme kann dann Worte formulieren, die die imitierte Person nie ausgesprochen hat und ist dabei von der Original-Stimme kaum zu unterscheiden.

Die Konsequenzen dieser Entwicklung sind nicht absehbar. Gefälschte Geständnisse in Prozessen, manipulierte Aussagen von Politikern oder Wirtschaftsführern, erlogene Interviewaussagen – all das liegt im Bereich des Möglichen. Die Entwicklung kommt zu einem Zeitpunkt, zu dem Manipulation für viele Menschen und auch Staaten ein politisches Werkzeug ist. Fake-News haben den US-Präsidentschaftwahlkampf massiv beeinflusst. Die russische Regierung manipuliert mit einer Propaganda-Einheit bereits heute systematisch Bilder. Auch Berufe dürften sich verändern, wenn die Software auf den Markt kommt. Nachrichten- und SynchronsprecherInnen sowie SchauspielerInnen könnten es als Erste merken. Man könnte gleich ganze Filmskripte neu einsprechen, was zeit- und ressourcensparend wäre. Auch werden wohl neue Aufgaben entstehen, etwa die der Ton-ForensikerIn, die untersucht, ob eine Aufnahme gefälscht oder authentisch ist. Auch hierbei könnte Software, so heißt es bei Adobe, helfen (Boie, Unerhört, SZ 08.11.2016, 1; Computer können ab jetzt eure Stimme perfekt imitieren, www.galileo.tv 14.11.2016).

Software bewertet Vertrauenswürdigkeit

Für Computer ist es eine gewaltige Herausforderung, Gesichter bzw. Bilder von Gesichtern zu interpretieren. Ein Team um Mel McCurrie von der amerikanischen Universität Notre Dame hat eine Software geschrieben, mit der das menschliche Gegenüber auf den ersten Blick per Algorithmus erfolgreich eingeschätzt werden soll. Sie bewertet die Vertrauenswürdigkeit von Personen auf einem Foto, ihr Al-

ter, den Intelligenzquotienten und wie dominant jemand wirkt.

Maschineller „Menschenkenntnis" scheiterte bisher daran, dass unklar war, wie Menschen zu ihren Urteilen über andere kommen. Es sind subtile Zeichen, Mimik, Blickrichtung der Augen, Haltung des Kopfes, die Signale geben, wie jemand bewertet wird. Auch Psychologen können dazu nur mutmaßen.

Um dieses Problem mit Computern zu „lösen", nutzten die Forschenden das Urteil Hunderter menschlicher Probanden als Basis. Sie zeigten BesucherInnen der Website testmybrain.org 6.000 Fotos von fremden Personen und die Probanden bewerteten die Bilder danach, wie alt, intelligent, dominant oder vertrauenswürdig die Personen ihnen erschienen. Mit der so gewonnenen Informationen trainierten die InformatikerInnen ein neuronales Netzwerk. Die Maschine lernte, zu einem ähnlichen ersten Eindruck von Fremden zu kommen wie Betrachtende, ohne zu wissen, wie dieser Eindruck zustande kommt. Der entwickelte Algorithmus bewertet nun auch neue Fotos.

Neuronale Netze lassen sich vielfältig nutzen. Ein ähnlicher Algorithmus hat nach der Aufarbeitung von 140.000 Bildern der Plattform Amazon gelernt, Bücher anhand ihres Covers in das richtige Genre einzuordnen. Ein Team der TU München bringt gerade einer Autosoftware bei, Baustellen auf der Straße zu erkennen. Dafür analysiert das System unzählige Verkehrssituationen und erschließt sich daraus selbst die Merkmale, die auf eine Baustelle hinweisen, wie etwa spitze Hütchen oder gelbe Markierungen.

Der Vertrauens-Algorithmus ist bislang Grundlagenforschung. Die US-InformatikerInnen zeigen aber mögliche Anwendungen: So überprüften sie die Software mit Fotos des Wikileaks-Chefs Julian Assange, des Whistleblowers Edward Snowden sowie der beiden Schauspieler, welche die Aktivisten in Filmen verkörpern. Der Algorithmus schätzte für beide Paare Vertrauenswürdigkeit, IQ, Alter und Dominanz fast identisch ein. Die Filmemacher hatten also aus Computersicht die Rollen gut besetzt (Behrens, Blick ins Innerste, SZ 11.11.2016, 1).

Chemotest bei Alltagsgegenständen

Aus den fettigen Abdrücken z. B. auf dem spiegelglatten Display eines Mobiltelefons lässt sich herauslesen, ob der Besitzer ein Mann oder eine Frau ist, welches Shampoo die Person zum Haarewaschen benutzt oder welche Medikamente sie wie gewissenhaft schluckt. Jeder Fingerabdruck hinterlässt nicht nur das Rillenmuster des Hautreliefs, sondern auch eine Vielzahl von Chemikalien, die von der Forensik identifiziert werden können. Ein internationales Forschungsteam hat eine Methode entwickelt, um die chemische Interpretation des Fingerschmiers zu verfeinern. In einem Fachjournal beschreibt das Team, wie sich aus den minimalen menschlichen Spuren auf glatten Oberflächen Rückschlüsse auf dessen Lebensweise ziehen lassen.

Amina Bouslimani von der University of California in San Diego beschreibt „Haut-assoziierte Lebensstil-Chemikalien", die sie und ihre KollegInnen auf Alltagsgegenständen entdeckt haben. Von 39 Probanden nahmen sie Abstriche von den Händen und vom Mobiltelefon. Allein anhand der chemischen Spuren auf der Geräteoberfläche konnten die Forschenden die Telefone ihren BesitzerInnen zuordnen. Wischproben von der Rückseite des Geräts lieferten dabei bessere Ergebnisse – mit einer Trefferquote von bis zu 85%. Bei der Überprüfung, was für Chemikalien sie auf den Oberflächen gefunden hatten, wies das Team Arzneimittelrückstände nach, unterschied verschiedene Kosmetikprodukte und identifizierte Umweltchemikalien. Bei einer Versuchsperson fanden sie Rückstände von Sonnen- und Feuchtigkeitscremes, Parfum und Insektenschutzmittel. Aus einem solchen chemischen Profil lasse sich folgern, dass die Spuren recht wahrscheinlich von einer Frau stammen, die sich viel im Freien aufhält. Bei einem anderen Probanden entdeckten die Chemiker mithilfe ihres Massenspektrometers, das Chemikalien anhand ihres Molekulargewicht unterscheiden kann, Spuren eines Antidepressivums und von Kunststoffweichmachern. In einem weiteren Fall spürten die Forschenden Haarwuchsmittel, Koffein und Hautcremes auf.

Bereits früher war es der Forensik gelungen, in Fingerabdrücken Chemikalienreste nachzuweisen. Auch Krankheiten hinterlassen eine eigene chemische Signatur im Fingerabdruck, die sich messen lässt. Damit die Methode aber wirklich nützlich wird, müssten Datenbanken mit Referenzwerten aufgebaut werden, in denen die Ermittlungsbehörden abgleichen können, was ihre Massenspektrometer in den Proben gefunden haben. Bouslimanis Team konnte bislang nur 2,3% der Chemikalien eindeutig identifizieren, weil sie nur diese in den bestehenden Datenbanken finden konnten. Bouslimani und ihre KollegInnen bezeichnen die Arbeit als Machbarkeitsstudie. Künftig könnte die Forensik-Methode helfen, sehr detaillierte Profile gesuchter TäterInnen zu erstellen. Ein Fingerabdruck ließe sich vielleicht fast so lesen wie ein Lebenslauf. Die ChemikerInnen sehen darin auch einen Weg, um etwa zu kontrollieren, ob PatientInnen ihre Medikamente regelmäßig einnehmen, ohne ihnen Blut abnehmen zu müssen, oder um die Belastung eines Menschen mit gesundheitsgefährdenden Chemikalien zu messen (Charisius, Das menschliche Schmierom, SZ 16.11.2016, 16).

Billig-Flatcam eröffnet neue Perspektiven der Bilderfassung

US-WissenschaftlerInnen der texanischen Rice-Universität/USA forschen an einem Kameraprinzip, das ohne Objektiv auskommt. Die sogenannte Flatcam ist flacher als eine Kreditkarte. Sie könnte im Internet der Dinge, in der Überwachungstechnik und Mikroskopie eingesetzt werden. Die sogenannte Flatcam, an der geforscht wird, hat ungefähr den Durchmesser einer Ein-Cent-Münze und ist flacher als eine Kreditkarte. Der Fotografie-Chip macht auch Foto- und Videoaufnahmen, wenn er verbogen wird. Die Mikrotechnik könnte bestehende Überwachungskameras ersetzen und diese quasi unsichtbar machen. Eingenäht in die Dienstkleidung von Polizisten wäre mehr Transparenz über deren Einsätze möglich. Für die mobile Technik der Zukunft, die möglicherweise biegbar sein wird wie das Reflex

Smartphone, könnte die Flatcam die Selfies liefern.

Der Professor für Computerwissenschaften Richard Baraniuk, Initiator des Projekts, erklärt den Grundgedanken: „Gewöhnliche Kamerasysteme fangen Licht durch ein Objektiv ein, das in einer gewissen Distanz zum Fotofilm oder der Sensorplatte stehen muss. Je kleiner die Kameras gebaut werden, desto geringer wird der Lichteinfall und letztendlich die Bildqualität. Die neue Technologie soll diese Einschränkung nun umgehen: Sein Team wolle „Objektive durch Algorithmen ersetzen“ und so die Fotografie revolutionieren: „Neben der Miniaturform hat die Flatcam den Vorteil sehr geringer Produktionskosten, da wenig Material und keine Montage benötigt werden“. Wenn sie einmal in Serie produziert werde, könnten die Stückkosten im Centbereich liegen.

Die Grundidee für die High-Tech-Entwicklung stamme aus den Anfängen der Fotografie. Schon vor fast 200 Jahren hat Joseph Nicéphore Nièpce nach dem Lochkameraverfahren die ersten Fotografien ohne Objektiv hergestellt. Dabei wird eine Holzkiste auf einer Seite mit einem stecknadelgroßen Loch versehen; auf der gegenüberliegenden Innenseite befindet sich das Fotomaterial, anfangs eine Zinnplatte, später Fotofilm. Dieses Material reagiert sensibel auf Licht und verfärbt sich je nach Stärke der Strahlen. Lässt man durch die Öffnung Licht einfallen, trifft es auf das Fotomaterial und projiziert darauf ein Abbild der Realität, das auf dem Kopf steht. Nièpce brauchte im Jahr 1826 für das erste Exemplar aus seinem Arbeitsraum acht Stunden und eine Distanz von rund einem halben Meter zwischen Loch und Platte.

Die Flatcam ist ein Lochkamera auf Mikroebene. Statt nur eines Lochs gibt es Hunderttausende, mikroskopisch kleine Öffnungen auf der einen Quadratzentimeter großen Kunststoffmaske. Die liegt in weniger als einem Millimeter Abstand vor einer Sensorplatine, der digitalen Version des Fotofilms. So entstehen gleichzeitig Hunderttausende Fotos, die jeweils nur einen oder zwei Pixel groß sind. Fügt man diese Pixel zusammen, ergibt das zunächst nur ein verschwommenes Bild. Weil der Abstand zwischen Öffnung und Sensor so gering ist, werden die Einfallstrahlen hinter der Maske nicht ausreichend gestreut. Die projizierten Lichtstrahlen sind zu dicht beieinander, um ein realitätsnahes Foto zu erzeugen. Die Wissenschaftler nennen das den Multiplex-Effekt.

Der Schlüssel zum erkennbaren Foto ist ein linearer Algorithmus, so Ashok Veeraraghavan, Assistenzprofessor und Mitglied des Forschungsteams: „Da wir mittlerweile sehr gut verstehen, wie sich Lichtstrahlen verhalten, können wir die dicht beieinander liegenden Informationen präzise dekodieren. Das System glättet sozusagen die einzelnen Aufnahmen und fügt sie zu einem Gesamtbild zusammen“. Dadurch entstehen digitale Mosaike mit 0,5 Megapixeln. Baraniuk erläutert das Prinzip: „Die algorithmische Berechnung wird bei uns sehr früh in den Prozess eingebunden, und als Hauptbestandteil der Sensorik genutzt. Dadurch können wir auf physische Sensorelemente wie das Objetiv verzichten und das Gerät verkleinern“. Diese Vermischung aus Hard- und Software sei auch in anderen Technologiebereichen zu erwarten. Auf den bisher produzierten Fotos mit dem Prototypen sind die Objekte gut erkennbar, bisher aber auch noch nicht mehr.

Die Einsatzmöglichkeiten sind vielfältig, so Baraniuk: „Die Flatcam soll vorerst nicht die Spiegelreflexkamera ersetzen. Wir sehen die Anwendung aktuell vor allem in der visuellen Interaktion zwischen Geräten.“ Es geht also zunächst um das sogenannte Internet der Dinge, die Vernetzung und den Datenaustausch von Geräten und Computern untereinander, z. B. in der Lagerhaltung: In die Wand eines Warenregals in einem Schuhladen wird die flache Kamera integriert und filmt den Lagerbestand eines gewissen Modells. Verändert sich der Bestand, leitet sie diese Information automatisch an das Lagerhaltungssystem weiter. Dies ist zwar heute schon mit konventioneller Technik möglich, aber zu weitaus höheren Kosten als es mit den Lensless Smart Sensors (LSS).

Gemäß dem LSS-Chefentwickler bei Rambus, Patrick Gill, können mit der Technik „jedem digitalen Gerät, unabhängig von seiner Größe, Augen hinzugefügt werden“. Besonders der Bereich Augmented Reality (AR) könne durch LSS Fortschritte machen. AR beschreibt Technologien, bei denen virtuelle Elemente in die menschliche Wahrnehmung der Realität einfließen. Die flächendeckende Anwendung der flachen Kameras liegt noch in der Zukunft. Fragen des Datenschutzes und der Datensicherheit werden dann relevant. Praktisch unsichtbare, fast kostenlose Kameras könnten zur weiteren exponenziellen Vermehrung visueller Daten führen.

Die Forschenden der Rice-Universität testen mittlerweile einen zweiten Prototypen, der Mikroskopbilder liefert, so Veeraraghavan: „Das Besondere dabei ist die Anwendung an Lebewesen zu geringen Kosten“. Mit einem Endoskop könne man die Kamera unter die Haut oder in den Körper von Menschen und Tieren bringen und, wenn nötig, dort für den Kontrollzeitraum auch lassen. Die sogenannte In-Vivo-Mikroskopie sei möglich, da die Flatcam nur wenig Licht benötige und bereits ab einem Objektabstand von 0,01 Zentimetern Bilder liefere. So könnten langfristige Tieruntersuchungen vereinfacht werden. Die Forschenden wollen mit der Kamera auch menschliche Zellen untersuchen und hoffen, zur billigen Krebsvorsorge beisteuern zu können.

Auf Hardware kann bei der Anwendung nicht verzichtet werden: Damit die Flatcam klarere Bilder liefert, muss die Sensorplatte feiner werden. In diesem Bereich gab es in den vergangenen Jahren keinen großen Fortschritt. Das von US-Institutionen geförderte Forscherteam um Baraniuk berichtet aber von großem Interesse seitens der Unternehmen. Sein Kollege Veeraraghavan ist aber optimistisch: „In den nächsten ein bis zwei Jahren wird die Flatcam von unterschiedlichen Organisationen auf Marktreife getestet“ (Ultraflache Kamera soll dem Internet das Sehen beibringen, www.golem.de 12.11.2016; Gluschak, Die Augen des Internets, SZ 09.11.2016, 26).

Studie: Passwörter sind leicht erratbar

Forschende der englischen Lancaster University und an chinesischen Hochschulen in Peking und Fujian kamen zu dem Ergebnis, dass Passwörter, die Nutzende einheitlich für verschiede-

ne Onlinekonten nutzen, durch Erraten leicht zu knacken sind, wenn nur wenige Informationen über die Betroffenen vorliegen. Sie starteten systematisch Testangriffe, wobei den Hackern mit wissenschaftlichem Interesse unterschiedlich viel Wissen über die auszuspähenden Nutzenden zur Verfügung stand. Überprüft wurde die Sicherheit von mehreren Tausend Internetkonten in Großbritannien und China. Dabei orientierten sich die Forschenden an den Vorgaben des National Institute of Standards and Technology in den USA, wonach es binnen 30 Tagen nicht mehr als 100 gescheiterte Versuche geben darf, sich in einen Account einzuloggen, Lagen persönliche Daten und gar das Passwort eines anderen Onlinekontos vor, gelang das Knacken mit 73% Wahrscheinlichkeit. Bei Nutzenden, die höhere Sicherheitsstandards anlegten, wurden immer noch 30% der Accounts gehackt. Ping Wang, Professor an der Peking University und Mitautor der Studie, verweist auf Datenlecks wie jüngst bei Yahoo oder LinkedIn, durch die Passwörter für Kriminelle zugänglich werden. Wegen des Sicherheitsrisikos müssten die Betroffenen durch unterschiedliche und wechselnde komplexe Passwortwahl die nötigen Vorkehrungen treffen (Der Spiegel 45/2016).

Authentifizierung per Hirnstromanalyse

US-Forschende haben ein biometrisches System entwickelt, das Hirnströme erkennen und künftig möglicherweise als Passwort zur Authentifizierung nutzen kann. Das System von John Chuang und seinem Team von der Universität von Kalifornien in Berkeley nutzt Hirnstromwellen. Arbeitet das Gehirn, erzeugt es ein charakteristisches Muster von Wellen, die mit Elektroenzephalographie-Elektroden (EEG) gemessen werden.

Die Idee zu einem Passthought, also Passgedanken, ist schon älter. Ein Passgedanke dürfte schwieriger zu fälschen sein als Finderabdrücke oder das Gesicht. Allerdings fehlte bisher ein praktikables Lesegerät, wie es z. B. ein EEG-Headset wie Mindwave von Neurosky ist. Chuang und seine KollegInnen haben Mindwave getestet und konnten ProbandInnen mit einer Genauigkeit von über 99% identifizieren. Als nächstes überlegten sie, ob sich dies in ein Gerät integrieren lässt, das viele ohnehin mit sich herumtragen. Sie bauten die Elektrode aus dem Headset aus und in einen Ohrhörer ein und testeten dieses rudimentäre System mit einer Gruppe aus zwölf ProbandInnen. Die Forschenden ließen sie jeweils zweimal fünf Denkaufgaben erledigen. Der EEG-Ohrhörer erkannte die Person mit einer Treffergenauigkeit zwischen 72 bis 80%. Das Team stellte sein System auf der Konferenz „Engineering in Medicine and Biology Society" vorgestellt. Um das System zu einem serienreifen Produkt weiterzuentwickeln, muss die Genauigkeit verbessert werden.

Probleme bereitet die Methode, wenn die NutzerIn nicht entspannt ist. So fanden Chuang und sein Sohn heraus, dass Sport einen starken Einfluss auf die Hirnaktivität hat: Nach einer Sportübung kann es eine Minute dauern, bis Hirnstromwellen wieder zu ihrem normalen Muster zurückkehren. Auch Stress, Alkohol, Koffein oder die Stimmung können die elektrischen Signale, die das Gehirn erzeugt, beeinflussen. Ein serienreifes System muss damit umgehen können. Sollte es robust genug sein, könnte schon das Nachdenken über ein vergessenes Passwort das Passwort sein (Pluta, Ich denke, also erkennt mich mein Computer, www.golem.de 01.09.2016).

Menschlicher Körper als Authentisierungs-Leitung

Forschenden ist es gelungen, Passwortschlüssel von einem Fingerabdruck-Scanner durch Fleisch, Blut und Knochen zu einer Empfangsstation, z. B. einer Türklinke, zu schicken. Das sei, so ihre Darstellung, deutlich langsamer als WiFi oder Bluetooth, aber auch deutlich sicherer.

Der Versuchsaufbau der Elektro- und Computeringenieure der University of Washington besteht darin, dass ein Proband ein Smartphone oder Laptop mit Fingerabdruck-Scanner in der einen Hand hält und mit der anderen nach einem Türgriff greift, der mit einem modifizierten Smartlock gekoppelt ist. Ein Finger wird auf den Sensor gelegt und das Schloss öffnet sich. Die Authentisierung mit der Schlüsselsequenz wird nicht vom Telefon oder Laptop über Wifi, NFC oder Bluetooth an das Smartlock gesendet, sondern fließt kodiert in einer elektromagnetischen Niederfrequenzwelle vom Scanner durch den Körper des Versuchsteilnehmers. Diese wird mit der sonst zum Scannen des Fingerabdrucks genutzten Technik generiert. Shyam Gollakota, Mitentwickler des Konzeptes, erklärt: „Fingerabdruck-Sensoren wurden bisher als Eingabegerät genutzt. Wir haben nun gezeigt, dass diese Scanner auch zum Senden von Informationen durch den Körper genutzt werden können."

Dabei sei der menschliche Körper mit seiner Zusammensetzung aus verschieden dichten und damit ungleich „leitfähigen" Stoffen als Datenleitung alles andere als ideal. Mit gerade einmal zwischen 25 und 50 Bit pro Sekunde werden die Login-Daten derzeit durch Fleisch, Blut und Knochen transportiert – was aber auch von der Leistungsfähigkeit der jeweils genutzten Sensoren abhängt. Körpergröße und -Umfang der Testpersonen oder mit welchem Körperteil sie den Türgriff berührt, all das hat hingegen nahezu keinen Einfluss. Die Tür ließe sich auch mit dem Fuß, Bauch oder Ohr öffnen.

Den EntwicklerInnen zufolge ist die sogenannte On-body-Transmission von Schlüsseldaten grundsätzlich deutlich sicherer als derzeitige NFC-, WiFi- oder Bluetooth-Systeme, so Mehrdad Hessar von der University of Washington: „Ich kann den Türknauf berühren und den Fingerabdruck-Sensor meines Telefons. Dabei werden die Daten nur durch den Körper geschickt, ohne etwas in die Luft abfließen zu lassen." Das System könne recht schnell eingesetzt werden, weil es sich mit vielen aktuellen Fingerabdruck-Scannern umsetzen ließe. Dabei sei der Einsatz nicht auf Smartlocks begrenzt, sondern könnte etwa auch zur Übertragung von Datenpaketen an medizinische Geräte wie Insulinpumpen oder andere Wearables genutzt werden (Förtsch, Forscher senden Login-Daten durch den Körper, www.wired.de 06.10.2016).

Rechtsprechung

EuGH

Anlasslose Vorratsdatenspeicherung ist grundrechtswidrig.

Der Europäische Gerichtshof (EuGH) in Luxemburg hat mit Urteil vom 21.12.2016 Regelungen zur anlasslosen Vorratsdatenspeicherung in Großbritannien für grundrechtswidrig erklärt und damit auch Vorlagen schwedischer und britischer Gerichte beantwortet (C-203/15, C-698/15)., Danach steht das Unionsrecht grundsätzlich einer nationalen Regelung entgegen, „die eine allgemeine und unterschiedslose Speicherung von Daten vorsieht“. Die Entscheidung wird Auswirkungen für das laufende Verfahren gegen die Neuregelung der Vorratsdatenspeicherung in Deutschland haben. Die Vorratsdatenspeicherung verlangt die Speicherung der Verbindungsdaten aller User, die bei der Telekommunikation, bei der Internet-Nutzung und im Mobilfunk anfallen, ohne konkreten Verdacht auf strafbare Handlungen, um auf Anforderung Strafverfolgern bei Ermittlungen zur Verfügung zu stehen.

Das EuGH-Urteil geht auf Klagen von Brexit-Minister David Davis u. a. gegen die britische Snooper´s Charter und des Anbieters Tele Sverige beim Oberverwaltungsgericht Stockholm, das dessen Aussetzung der Datenspeicherung absegnen lassen wollte, zurück. Im Urteil zu den zusammengezogenen Verfahren aus England und Schweden wird klargestellt, dass die Gesamtheit von anlasslos gespeicherten Daten „sehr genaue Schlüsse auf das Privatleben der Personen zu, deren Daten auf Vorrat gespeichert werden“, zulässt. Dies ermögliche die Erstellung eines Profils, „das im Hinblick auf das Recht auf Privatsphäre eine genauso sensible Information darstellt wie der Inhalt der Kommunikation selbst“. Daher handele es auch um einen schwerwiegenden Grundrechtseingriff, wenn ohne Anlass Verkehrs- und Standortdaten gespeichert würden. Es fehle ein Zusammenhang zwischen den anlasslos gespeicherten Daten und einer Bedrohung der öffentlichen Sicherheit. Er beschränke sich „nicht auf die Daten eines Zeitraums und/oder eines geografischen Gebiets und/oder eines Personenkreises, der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte“. Eine Vorratsdatenspeicherung können ausnahmsweise zulässig sein; sie dürfe aber nicht – wie in Schweden und Großbritannien – zur Regel werden. Gemäß den Regelungen in Schweden und in Großbritannien waren die Verkehrs- und Standortdaten sechs bzw. zwölf Monate zu speichern. Eine solche Regelung überschreite die „Grenzen des absolut Notwendigen“. Der EuGH wies darauf hin, was aus seiner Sicht noch möglich ist: eine gezielte, aus gegebenem Anlass erfolgende Speicherung. Dafür müssen die Gesetzgeber allerdings eine Reihe von Maßgaben erfüllen. Der Zugang muss in der Regel – außer im Notfall – von einem Richter abgesegnet werden und die Daten sind in Europa zu speichern.

Das Urteil wirft auch ein Licht auf neue Verfahren beim Bundesverfassungsgericht (BVerfG). Erst vergangene Woche hatte DigitalCourage ein neues Massenverfahren mit 33.000 Mitunterzeichnenden angestrengt. Sollte das BVerfG in seiner Entscheidung hinter der Rechtsprechung des EuGH zurückbleiben, könnten sich die Kläger aufgefordert fühlen, selbst den Weg nach Luxemburg zu beschreiten.

Rechtsanwalt Meinhard Starostik, der für die Organisation DigitalCourage eine große Gruppe von Verbänden und 33.000 Einzelbeschwerdeführerinnen vor dem BVerfG vertritt, meinte, das EuGH-Urteil setze „klare Grenzen, die das deutsche Gesetz bereits bei der Erhebung der Daten überschreitet“. Beispielsweise müsse eine gezielte, und daher noch zulässige, Speicherung auf die „Bekämpfung schwerer Straftaten“ begrenzt werden und grundsätzlich die Speicherung von Daten auf das „absolut Notwendige hinsichtlich der Kategorien der zu speichernden Daten, der erfassten Kommunikationsmittel, der betroffenen Personen und der vorgesehenen Dauer“ beschränkt werden. Außerdem dürften von vornherein nur Personen ins Visier genommen werden, „deren Daten einen unmittelbaren oder zumindest mittelbaren Zusammenhang mit schweren Straftaten haben“. Beziehungsweise es gelte, einen bestimmten geographischen Umkreis für eine Speichermaßnahme zu ziehen. Starostik hofft, „dass das Bundesverfassungsgericht im Lichte seiner eigenen Rechtsprechung und dieses klaren Urteils des EuGH nunmehr kurzfristig das deutsche Gesetz für verfassungswidrig erklärt, damit die Speicherung am 1. Juli 2017 erst gar nicht beginnt“.

Volker Tripp, politischer Geschäftsführer des Vereins Digitale Gesellschaft, erklärte mit Blick auf die Umsetzung der Vorratsdatenspeicherung in Deutschland: „Mit seinem heutigen Urteil zur Vorratsdatenspeicherung macht der Europäische Gerichtshof allen Sicherheitsesoterikern und Überwachungsfanatikern einen dicken Strich durch die Rechnung. [...] Nun muss auch Deutschland reagieren und die erst im vergangenen Jahr verabschiedete Neuauflage der Vorratsdatenspeicherung ein für alle Mal auf den Müllhaufen der Geschichte verbannen.“

Oliver Süme, Vorstand Politik & Recht des eco-Verbands der Internetwirtschaft begrüßte ebenso die Entscheidung: „Die Richter haben ihre Chance einer weiteren Grundsatzentscheidung genutzt: Die Mitgliedstaaten dürfen keine anlasslose und allgemeine Vorratsdatenspeicherung festlegen. Damit sehen wir unsere wiederholt geäußerten Bedenken bestätigt.“ Es sei äußerst zweifelhaft, ob das deutsche Gesetz zur anlasslosen Vorratsdaten-

speicherung in seiner konkreten Ausgestaltung den strengen materiellen und prozeduralen Anforderungen des Gerichtshofs genügt. „Wir brauchen jetzt dringend ein Moratorium, um die Umsetzung der Vorratsdatenspeicherung in Deutschland zu stoppen; andernfalls laufen die Unternehmen Gefahr ein europa- und verfassungsrechtswidriges Gesetz umsetzen zu müssen und damit Gelder in Millionenhöhe in den Sand zu setzen.“

Schon mit einem Urteil vom 08.04.2014 hatte der EuGH enge Grenzen gezogen und klar gemacht, dass eine völlig anlasslose Speicherung von Verkehrsdaten als grundsätzlich grundrechtswidrig zu betrachten ist (C-293/12 u. C-594/12). Von Seiten der Opposition in Deutschland, von den Grünen, ebenso wie auch von den Piraten und aus dem liberalen Lager kamen bereits mehrere Forderungen, der deutsche Gesetzgeber möge sich bitte endgültig von einer anlasslosen Generalspeicherung verabschieden.

Das Urteil erging zu einem heiklen Zeitpunkt: zwei Tage nach dem terroristischen Anschlag in Berlin, der Sicherheitsbehördenvertreter und Politiker erneut dazu brachte, eine Ausweitung der vor dem BVerfG angefochtenen Vorratsdatenspeicherung zu fordern. Das Urteil lässt den Mitgliedstaaten einen Spielraum und macht Ermittler nicht blind. Es räumt aber auf mit dem Mythos der Unverzichtbarkeit der TK-Vorratsdatenspeicherung. Die Hälfte der europäischen Regierungen war in dem Verfahren vertreten, doch konnten sie das Gericht nicht von der Effizienz der Speicherei überzeugen. Valide, übergreifende Studien sucht man weiterhin vergebens. Eine weitere Dimension des Urteils liegt darin, dass sich in einigen Staaten Osteuropas derzeit eine radipe Erosion des Rechtsstaats vollzieht. In den Händen von Autokraten kann ein riesiger Datenpool, der nur zur Bekämpfung schwerer Kriminalität genutzt werden dürfte, zur Infrastruktur einer Massenüberwachung werden (Ermert, Europäischer Gerichtshof bekräftigt: Anlasslose Vorratsdatenspeicherung ist illegal Update, www.heise.de 21.12.2016; Janisch, Das Privatleben muss geschützt bleiben, Urteil gegen Autokraten, SZ 22.12.2016, 1, 4).

BVerfG

Vertraulichkeitszusage gegenüber USA geht vor parlamentarisches Untersuchungsrecht

Mit Beschluss vom 13.10.2016 hat der Zweite Senat des Bundesverfassungsgerichts (BVerfG) entschieden, dass die Bundesregierung (BReg) die NSA-Selektorenlisten, mit der der Bundesnachrichtendienst (BND) für die Vereinigten Staaten von Amerika (USA) Telekommunikationsüberwachung durchführt, nicht an den NSA-Untersuchungsausschuss des Deutschen Bundestags herausgeben muss (2 BvE 2/15). Zwar umfasst das Beweiserhebungsrecht des Untersuchungsausschusses dem Grunde nach auch die NSA-Selektorenlisten, doch berührten diese zugleich Geheimhaltungsinteressen der USA und unterlägen deshalb nicht der ausschließlichen Verfügungsbefugnis der BReg. Eine Herausgabe unter Missachtung einer zugesagten Vertraulichkeit und ohne Einverständnis der USA würde die Funktions- und Kooperationsfähigkeit der deutschen Nachrichtendienste und damit auch die außen- und sicherheitspolitische Handlungsfähigkeit der BReg nach verfassungsrechtlich nicht zu beanstandender Einschätzung der Regierung erheblich beeinträchtigen. Das Geheimhaltungsinteresse der Regierung überwiege insoweit das parlamentarische Informationsinteresse, zumal die BReg dem Vorlageersuchen in Abstimmung mit dem NSA-Untersuchungsausschuss so präzise, wie es ohne eine Offenlegung von Geheimnissen möglich war, Rechnung getragen habe. Sie hat insbesondere Auskünfte zu den Schwerpunkten der Zusammenarbeit von BND und National Security Agency (NSA), zum Inhalt und zur Zusammenstellung der Selektoren, zur Filterung der Selektoren durch den BND sowie zur Anzahl der abgelehnten Selektoren erteilt. Insofern bestehe nicht die Gefahr des Entstehens eines kontrollfreien Raumes und damit eines weitgehenden Ausschlusses des Parlaments von relevanter Information.

Faktischer Hintergrund des Beschlusses ist die Kooperation bei der Fernmeldeaufklärung zwischen BND und der US-amerikanischen NSA eine Kooperation, wobei der BND die aus einem Internetknotenpunkt ausgeleiteten Daten nach von der NSA definierten Merkmalen, den sogenannte Selektoren, auswertet. Nachdem im Sommer 2013 in der Folge der Snowden-Enthüllungen bekannt geworden war, dass auch EU-Vertretungen und deutsche Grundrechtsträger von der Überwachung durch BND und NSA betroffen seien, setzte der Deutsche Bundestag im März 2014 den sogenannten NSA-Untersuchungsausschuss ein. Dieser verlangte von der BReg die Herausgabe sämtlicher Beweismittel, die Auskunft darüber geben, welche Erkenntnisse beim BND darüber vorliegen, inwiefern die NSA im Rahmen der Kooperation Aufklärung gegen deutsche Ziele oder deutsche Interessen betrieben hat. Die BReg legte daraufhin Beweismaterial vor. Die NSA-Selektorenlisten verweigerte sie aber mit der Erklärung, eine Herausgabe an den Untersuchungsausschuss ohne Einverständnis der USA verstoße gegen die gegenseitig zugesagte Vertraulichkeit und würde die internationale Kooperationsfähigkeit Deutschlands beeinträchtigen. Stattdessen wurde eine „Vertrauensperson“ bestellt: Der Ex-Bundesverwaltungsrichter Kurt Graulich wertete die Liste aus. In seinem Bericht warf er den USA Ende Oktober 2015 gravierende Verstöße gegen vertragliche Vereinbarungen vor.

Im Organstreitverfahren begehrten daraufhin die Fraktionen im Bundestag „Die Linke“ und „Bündnis 90/Die Grünen“ sowie deren Mitglieder im NSA-Untersuchungsausschusses Martina Renner und Konstantin von Notz die Feststellung, dass die BReg und der Chef des Bundeskanzleramtes durch die Ablehnung der Herausgabe das Beweiserhebungsrecht des Bundestages aus Art. 44 GG verletzt haben.

Das BVerfG befand, dass sei der Untersuchungsausschuss als Hilfsorgan des Deutschen Bundestages gem. Art. 44 Abs. 1 Satz 1 GG zwar befugt sei, im Rahmen seines Untersuchungsauftrages diejenigen Beweise zu erheben, die er für erforderlich hält. Doch unterläge dieses Beweiserhebungsrecht auch Grenzen, die ihren Grund aber im Verfassungsrecht haben müssen. Dies könnten nicht völkerrechtliche Verpflichtungen sein, da diese keinen Verfassungsrang besit-

zen. Etwas anderes gelte für den Gewaltenteilungsgrundsatz. Als Gebot der Unterscheidung zwischen gesetzgebender, vollziehender und rechtsprechender Gewalt diene er einer funktionsgerechten und aufgabenadäquaten Zuordnung hoheitlicher Befugnisse zu unterschiedlichen Trägern öffentlicher Gewalt.

Der Staat sei von Verfassungs wegen verpflichtet, das Leben, die körperliche Unversehrtheit und die Freiheit des Einzelnen zu schützen, etwa indem er terroristischen Bestrebungen entgegen tritt. Die Bereitstellung wirksamer Aufklärungsmitteln zu ihrer Abwehr sei ein legitimes Ziel und für die demokratische und freiheitliche Ordnung von großem Gewicht. Zur Effektivierung der Beschaffung und Auswertung von Informationen von außen- und sicherheitspolitischer Bedeutung arbeiten die deutschen Nachrichtendienste mit ausländischen Nachrichtendiensten zusammen. Grundlage dieser Zusammenarbeit sei die Einhaltung von Vertraulichkeit. Es obliege der BReg, hierfür völkerrechtliche Verpflichtungen als Teil der Außen- und Sicherheitspolitik der Initiativ- und Gestaltungsbefugnis der BReg einzugehen.

Die Verweigerung der Vorlage der NSA-Selektorenlisten verletze nicht das Beweiserhebungsrecht des Deutschen Bundestages aus Art. 44 GG. Durch die Einsetzung einer sachverständigen Vertrauensperson und deren gutachterliche Stellungnahme sei der Informationsrecht des Bundestags nicht erfüllt worden. Doch stehe einer weitergehenden Beweiserhebung das Interesse der Regierung an funktionsgerechter und organadäquater Aufgabenwahrnehmung entgegen. Die USA hätten deutlich gemacht, dass der Untersuchungsausschuss als Außenstehender anzusehen und die Herausgabe der NSA-Selektorenlisten an ihn nicht vom Übermittlungszweck umfasst sei. Sie habe der BReg vermittelt, dass die Herausgabe der NSA-Selektorenlisten die Funktions- und Kooperationsfähigkeit der Nachrichtendienste und damit auch die außen- und sicherheitspolitische Handlungsfähigkeit der Bundesregierung erheblich beeinträchtigen würde. Angesichts einer solchermaßen konkretisierten Gefährdungslage für die äußere und innere Sicherheit der Bundesrepublik Deutschland seien zugleich im Staatswohl gründende Geheimhaltungsinteressen berührt. Diese tatsächliche und rechtliche Wertung des Verhältnisses zu ausländischen Nachrichtendiensten und Partnerstaaten unterliege angesichts des Einschätzungs- und Prognosespielraums der BReg nur einer eingeschränkten verfassungsgerichtlichen Kontrolle. Selbst wenn man im Hinblick auf die Folgenschwere eines Vertrauensbruches relativierend davon ausginge, dass sich die Herausgabe der Selektorenlisten an den Untersuchungsausschuss nur vorübergehend auf den Umfang des internationalen Informationsaustauschs auswirkte, wären hiermit eine nicht hinzunehmende temporäre Beeinträchtigung der Funktionsfähigkeit der Nachrichtendienste und damit eine Sicherheitslücke naheliegend.

Das Interesse an der Erhaltung der außen- und sicherheitspolitischen Handlungsfähigkeit der Bundesregierung überwiegt das Recht des Untersuchungsausschusses auf Herausgabe der NSA-Selektorenlisten. Soweit es um die Herausgabe der Selektorenlisten und damit um die konkrete Benennung, also die namentliche Erwähnung der als Erfassungsziele betroffenen natürlichen oder juristischen Personen sowie Institutionen und staatlichen Einrichtungen geht, sei deren Kenntnis eher von allgemeinem politischem Interesse und für die Erfüllung des Untersuchungsauftrages und damit für die parlamentarische Kontrolle des Regierungshandelns nicht in einem Maße zentral, um gegenüber den Belangen des Staatswohls und der Funktionsfähigkeit der Regierung Vorrang zu beanspruchen

Grünen-Obmann Konstantin von Notz kritisierte: „Weite Teile der jahrelangen, rechtswidrigen BND-Praxis werden jetzt im Dunkeln bleiben.“ Die Obfrau der Linken, Martina Renner, ergänzte, die Entscheidung signalisiere, „dass die Geheimdienste weiter machen können, was sie wollen, ungestört von parlamentarischer Kontrolle. Wieder einmal müssen die Rechte des Parlaments gegenüber den Geheimdienstinteressen zurücktreten.“ Regierungskoalitionäre äußerten sich dagegen zufrieden, etwa der Ausschussvorsitzende Patrick Sensburg (CDU): „Es gibt Dinge, die geheim bleiben müssen. Sonst können die Geheimdienste nicht arbeiten“. Voll bestätigt fühlte sich auch Nina Warken, die Obfrau der Unionsfraktion im Untersuchungsausschuss: „Nun haben wir es schwarz auf weiß, dass wir mit dem eingeschlagenen Weg das Aufsichtsrecht des Parlaments und das Sicherheitsinteresse des Staates in einen klugen Ausgleich gebracht haben“ (PM BVerfG ,Nr. 84/2016 v. 15.11.016, Im besonderen Fall der NSA-Selektorenlisten hat das Vorlageinteresse des Untersuchungsausschusses zurückzutreten; NSA-Selektorenliste bleibt geheim: Opposition enttäuscht über Karlsruher Urteil, www.heise.de 15.11.2016).

BGH

Antrag auf Anhörung von Snowden muss – erst später – behandelt werden

Mit Beschluss vom 11.11.2016 entschied eine Ermittlungsrichterin des Bundesgerichtshofs (BGH), dass der NSA-Untersuchungsausschuss des deutschen Bundestags noch einmal über Teile eines Antrags abstimmen muss, mit dem die Bundesregierung aufgefordert werden soll, die Voraussetzungen für eine Vernehmung des Zeugen Snowden in Deutschland zu schaffen (1 BGs 125/16). Damit sind die Chancen, Whistleblower Edward Snowden als Zeuge vor den Untersuchungsausschuss nach Berlin zu holen, für die Oppositionsfraktionen der Grünen und Linken gestiegen, die die „pass- und ausländerrechtliche Ermöglichung von Einreise und Aufenthalt sowie Zusage eines wirksamen Auslieferungsschutzes“ gefordert hatten. Eine Aussage dahingehend, dass die Bundesregierung verpflichtet ist, dem durch den Untersuchungsausschuss zu beschließenden Ersuchen nachzukommen, ist mit diesem Beschluss nicht verbunden. Bisher hatte die Ausschussmehrheit sich daran gehindert gesehen, die Regierung überhaupt nur um Amtshilfe zu bitten. Sollte der Antrag weiterhin von einem Viertel der Ausschussmitglieder unterstützt werden, müsse der Ausschuss zumindest mehrheitlich zustimmen, entschied die Ermittlungsrichterin. Die Große Koalition kann das durch ihre Mehrheit

in dem Untersuchungsausschuss auch nicht verhindern. Die Bundesregierung hatte mehrfach angedeutet, möglicherweise müsse Snowden an die USA ausgeliefert werden, sobald er deutschen Boden betrete. Snowdens Anwalt Wolfgang Kaleck hält seine Auslieferung für juristisch nicht zulässig. Was Snowden vorgeworfen wird, sei eindeutig eine Straftat mit politischem Charakter; nach dem Rechtshilfeabkommen mit den USA wird in diesen Fällen nicht ausgeliefert. Die BGH-Ermittlungsrichterin stellte aber klar: „Die Entscheidung, ob von einer Auslieferung abgesehen werden kann oder diese rechtlich geboten ist, obliegt der Bundesregierung, nicht dem Ausschuss".

Mit Beschluss vom 21.12.2016 entschied dann der BGH auf die Beschwerde der Regierungsfraktionen gegen den o. g. Beschluss hin, dass der NSA-Ausschuss vorerst nicht erneut über die Befragung von Edward Snowden abstimmen darf (3 ARs 20/16). Eine Entscheidung im Hauptsacheverfahren müsse zunächst abgewartet werden.

Eine mögliche Befragung des inzwischen 33-jährigen Whistleblowers in Berlin sorgt schon lange für Zündstoff. Der ehemalige NSA-Mitarbeiter Snowden hatte im Juni 2013 die massenhafte Internet-Überwachung durch die NSA, deren britischen Partner GCHQ und andere Geheimdienste enthüllt. Auch Deutschland ist davon betroffen, was der Auslöser für die Einrichtung des parlamentarischen Untersuchungsausschusses war. Der NSA-Untersuchungsausschuss entschied bereits 2014, Snowden, der auf seiner Flucht Asyl in Russland bekam, als Zeugen zu hören. Das wurde bisher nicht umgesetzt. Grüne und Linke halten der Bundesregierung vor, eine Entscheidung dazu in die Länge zu ziehen.

Im Dezember 2014 waren Grüne und die Linke mit einem juristischen Vorstoß beim Bundesverfassungsgericht (BVerfG) gescheitert, um die Befragung Snowdens durchzusetzen (DANA 1/2015, 48 f.). Das BVerfG in Karlsruhe hatte die Klage abgelehnt und auf die Zuständigkeit des BGH verwiesen. Die Koalitionspartner Union und SPD hatten sich gegen eine Vernehmung auf deutschem Boden gestellt und waren damit den außenpolitischen Bedenken der Bundesregierung gefolgt. Diese fürchtet eine schwere Belastung der Beziehungen zu den USA, falls der frühere Geheimdienstmitarbeiter nach Deutschland kommen würde. Für Grüne und Linke ist eine Vernehmung per Video oder in Moskau dagegen nicht gleichwertig zu einer persönlichen Befragung in Berlin.

Martina Renner, Linken-Obfrau im Untersuchungsausschuss, sieht „eine große Chance für den Bundestag, mit dem Zeugen Edward Snowden wesentliche Fragen der Überwachungspraxis der USA zu klären". Das sei lange überfällig. „Die Bundesregierung steht jetzt vor der Bewährungsprobe. Sie darf sich den Interessen der Geheimdienste nicht unterwerfen" (PE BGH 209/2016 v. 21.11.2016, Bundesgerichtshof verpflichtet „NSA-Untersuchungsausschuss" zum Amtshilfeersuchen an die Bundesregierung; BGH-Entscheidung: NSA-Ausschuss darf Edward Snowden vorladen, www.heise.de 21.11.2016; Janisch, Ein Zeuge namens Snowden, SZ 22.11.2016, 1, 5; BGH-Beschluss zu Snowden, SZ 22.12.2016, 5).

BGH

AGB können zur Untersuchung bei Versicherungsvertragsärzten verpflichten

Mit Urteil vom 13.07.2016 gab der Bundesgerichtshof (BGH) eine Antwort darauf, ob Versicherungsnehmer einer Versicherung es erdulden müssen, von einem von der Versicherung bestimmten Arzt untersucht zu werden, wenn die Untersuchung klären soll, ob die Versicherung leisten muss oder nicht (IV ZR 292/14). Das Urteil lässt bei entsprechender Vertragsgestaltung regelmäßig die Persönlichkeitsrechte zurücktreten, insbesondere beim Outsourcing der Verarbeitung von Gesundheitsdaten.

Eine Versicherte behauptete unter Rückenschmerzen zu leiden und suchte verschiedene Ärzte auf, die ihr Therapien wie Massage oder Krankengymnastik verschrieben. Nach ihrer Auffassung führten diese aber zu keinem dauerhaften Erfolg. Sie kam nun auf die Idee, als Tochter einer Physiotherapeutin und privat Krankenversicherte, sich von ihrer Mutter behandeln zu lassen und bei der Versicherung neben den Untersuchungskosten anderer Ärzte auch Mutters Behandlungskosten in Rechnung zu stellen. Die Zahlung wurde durch die Versicherung verweigert. In den AGB hieß es explizit, dass „keine Leistungspflicht besteht für Behandlungen durch (…) Eltern".

Die Vorinstanzen zum BGH gaben der Versicherung insoweit Recht, dass sie die Rechnungen der Mutter aufgrund der eindeutigen Klausel und nachvollziehbaren Möglichkeit des Versicherungsbetrugs nicht begleichen musste. Der BGH setzte sich damit nicht mehr vertieft auseinander. Bezüglich der anderen Rechnungen forderte die Versicherung die Tochter auf, sich von einem von der Versicherung ausgewählten Arzt bzgl. der Rückenbeschwerden untersuchen zu lassen, um die Leistungspflicht der Versicherung zu prüfen. Hierzu hieß es in den AGBs, dass „der Versicherungsnehmer (…) auf Verlangen des Versicherers jede Auskunft zu erteilen [hat], die zur Feststellung des Versicherungsfalles oder der Leistungspflicht des Versicherers und ihres Umfanges erforderlich ist. (…) Auf Verlangen des Versicherers ist die versicherte Person verpflichtet, sich durch einen vom Versicherer beauftragten Arzt untersuchen zu lassen".

Dieser Aufforderung kam die Tochter nicht nach, woraufhin die Versicherung die Rechnungen im Rahmen der Rückenbeschwerden auch nicht beglich. Die Versicherte monierte, dass die in den AGB niedergelegte Verpflichtung zu einer Untersuchung durch einen von der Versicherung ausgewählten Arzt unzulässig sei. Sie wies auf § 213 Versicherungsvertragsgesetz (VVG) hin, der die Erhebung von Gesundheitsdaten nur u. a. von Ärzten und nur nach Einwilligung der betroffenen Person zulässt. Gemäß ihrem Recht auf informationelle Selbstbestimmung habe sie grundsätzlich das Recht, über die Preisgabe und Verwendung von Daten selbst zu bestimmen.

Der BGH wies die Bedenken der Versicherten zurück und erklärte § 213 VVG für nicht für anwendbar. Zudem werde das Recht auf informationelle Selbstbestimmung nicht verletzt. § 213 VVG sei nicht einschlägig an, da die Regelung davon ausgehe, dass ein Dritter die Gesundheitsdaten erhebe und da-

mit eine eigenständige verantwortliche Stelle. Im vorliegenden Fall sei der Arzt aber gar keine verantwortliche Stelle, sondern ein Auftragnehmer der Versicherung, da er den Weisungen der Versicherung unterworfen sei und eine „reine Hilfsfunktion“ habe. Daher sei „der Arzt (…) mithin nicht als „Herr der Daten“, sondern lediglich als „verlängerter Arm“ des Versicherers anzusehen…“. Die von dem BGH herangezogene Literatur stellt hier auch darauf ab, dass der beauftragte Arzt keinen eigenen Zweck mit der Untersuchung der Versicherten verfolge, was ebenfalls für eine Auftragsdatenverarbeitung spräche.

Auch sei eine Verletzung des informationellen Selbstbestimmungsrechts der Versicherten nicht gegeben. Man müsse dieses Recht der Versicherten mit dem Grundrecht der Berufsfreiheit der Versicherung abwägen. Das Recht auf Berufsfreiheit sei höher zu gewichten, da die Versicherung im Interesse der Versicherungsgemeinschaft ungerechtfertigte Versicherungsleistungen vermeiden und daher die Möglichkeit haben müsse, den Eintritt des Versicherungsfalls zu überprüfen.

Gemäß diesem Urteil kann eine Versicherung mit einem Berufsgeheimnisträger einen Vertrag zur Auftragsdatenverarbeitung nach § 11 BDSG schließen und dann die von diesem erhobenen Daten nutzen. § 203 StGB regelt dagegen, dass ein „unbefugtes Offenbaren“ von Geheimnissen, die einem Berufsgeheimnisträger wie einem Arzt anvertraut worden sind, bestraft wird. Unbefugt ist die Offenbarung nur dann nicht, wenn der Arzt die Einwilligung des Betroffenen einholt. Von einer freiwillig erklärten Einwilligung konnte im konkreten Fall keine Rede sein. Der BGH befasste sich Urteil überhaupt nicht mit dieser Frage der Freiwilligkeit.

Die Versicherung gibt den Versicherten in ihren AGB die Obliegenheit auf, sich ggf. von einem Arzt untersuchen zu lassen. Zwar werden aus strafrechtlicher Sicht keine hohen Anforderungen an die Form der Einwilligung gestellt. Hier reicht eine konkludente Einwilligung. So gesehen kann auch eine Vereinbarung in den AGB, die den Versicherten zu einer Untersuchung bei einem Arzt verpflichtet, damit die Versicherung den Leistungsumfang abschätzen kann, eine Einwilligung darstellen. Allerdings wird diese Erklärung nicht gegenüber dem Arzt abgegeben. Der BGH scheint davon auszugehen, dass die Erklärung über den Umweg über die Versicherung auch für den Arzt Gültigkeit hat und so die Schweigepflicht des Arztes gegenüber der Versicherung aufhebt. Auch auf die Notwendigkeit einer besonderen Hervorhebung solch einer Einwilligung, wie das BDSG sie vorsieht, geht der BGH nicht ein.

Demgegenüber verlangen Aufsichtsbehörden für den Fall einer Auftragsdatenverarbeitung eine ausdrückliche Einwilligung von Patienten gegenüber dem Berufsgeheimnisträger, wenn eine Auftragsdatenvereinbarung vorliegt. Auch damit setzt sich der BGH in dem Urteil nicht auseinander. Nach dem Urteil würde also eine Vereinbarung in den AGB genügen, um eine wirksame und gemäß § 203 StGB konforme Auftragsdatenverarbeitung zu begründen. Auch wäre die Belehrung über ein Widerrufsrecht einer Einwilligung, wie sie das BDSG fordert, nicht erforderlich. Dass hier eine eigenständige Aufgabenwahrnehmung durch den Arzt erfolgt, die schon definitionsgemäß keine Auftragsdatenverarbeitung sein kann, wird vom BGH auch nicht erörtert.

Der meint vielmehr schlicht, dass Interessen eines Versicherungsnehmers regelmäßig zurücktreten müssten, wenn eine Versicherung prüfen möchte, ob Leistungen gerechtfertigt sind. Das Argument, dass die Versicherungsgemeinschaft geschützt werden müsse, lässt sich auf jegliche Art von Versicherung anwenden. Da hier besonders sensible Gesundheitsdaten erhoben und dann abgefragt werden können, könnten erst recht andere Daten durch einen beauftragten Externen im Auftrag der Versicherung erhoben und verarbeitet werden (z. B. Gutachter), ohne dass es einer ausdrücklichen Einwilligung bedarf. Dies würde z. B. auch legitimieren, im Rahmen eines Prämienprogramms einer Krankenversicherung Daten von Wearables auf der Basis von AGB und ohne ausdrückliche Einwilligung der Versicherten zu erheben. Auch würde genügen, dass Berufsgeheimnisträger (neben Ärzten sind dies bspw. auch Anwälte, Apotheker oder Steuerberater) in ihren AGB eine Vereinbarung aufnehmen, die sie dazu berechtigt, externe Dienstleister und Cloudservices im Rahmen einer Auftragsdatenvereinbarung zu beschäftigen. Eine Belehrung über ein Widerrufsrecht oder dass diese Einwilligung besonders hervorgehoben sein muss, wäre nach dem Urteil des BGH nicht notwendig. Dies steht im Widerspruch zur bisherigen Rechtsprechung des Bundesverfassungsgerichts, die verbietet, dass ein faktisch überlegener Vertragspartner einen Vertragsinhalt zu existenziellen Fragen des persönlichen Lebens – wozu derartige Versicherungen gehören – einseitig bestimmt (BVerfG U. v. 23.10.2016, 1 BvR 2027/02). Der BGH geht zwar auf diese Rechtsprechung ein, erklärt aber das Selbstbestimmungsrecht der Versicherten für weniger gewichtig als die Interessen der Versicherung (Rossow, www.datenschutz-notizen.de; juris.bundesgerichtshof.de).

BVerwG

Journalisten- und Anwaltsklage gegen BND teilweise abgewiesen

Das Bundesverwaltungsgericht (BVerwG) in Leipzig hat mit Urteilen vom 14.12.2016 die Zulässigkeit von Klagen verneint, mit denen sich ein Rechtsanwalt und der Verein „Reporter ohne Grenzen“ gegen die strategische Überwachung von E-Mail-Verkehr durch den Bundesnachrichtendienst (BND) wehrte. Die Klagen gegen die Speicherung und Nutzung von Metadaten in dem System VERAS des BND wurden zur weiteren Verhandlung und Entscheidung abgetrennt (6 A 9.14, 6 A 2.15). Das BVerwG ist für Klagen gegen den BND in erster und letzter Instanz zuständig.

Nach dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Art. 10-Gesetz) ist der BND im Rahmen seiner Aufgaben berechtigt, die Telekommunikation (TK) zu überwachen und aufzuzeichnen. Bei der strategischen Fernmeldeüberwachung werden internationale TK-Beziehungen anhand vorher festgelegter Suchbegriffe durchsucht. Die Kläger haben die Feststellung beantragt, dass der BND durch die Überwachung von E-Mail-Verkehr im Rahmen der strategischen Fernmeldeüberwachung in den Jahren 2012 bzw. 2013 ihr Fernmel-

degeheimnis aus Art. 10 GG verletzt hat. Das BVerwG wies die Klagen insofern als unzulässig ab und bestätigte damit eine Entscheidung aus dem Jahr 2014 zu einem anderen Überwachungszeitraum gegen Rechtsanwalt Niko Härting im Ergebnis. Härting vertrat im konkreten Verfahren einen Kläger. In der Verhandlung erklärte der Vorsitzende: „Das Bundesverwaltungsgericht ist kein öffentliches Tribunal, das die Tätigkeit des BNDs im allgemeinen und umfassend zu beurteilen hat.“ Vielmehr sei es seine Aufgabe zu entscheiden, ob eine bestimmte Maßnahme der Exekutive die individuellen Rechte eines Klägers verletze. Dies setze ein konkretes Rechtsverhältnis voraus.

Das BVerwG meinte, ein für eine Feststellungsklage nötiger auf konkreter, den jeweiligen Kläger betreffenden Sachverhalt sei nicht feststellbar gewesen. Unter den TK-Verkehren, die der BND in den Jahren 2012 bzw. 2013 als nachrichtendienstlich relevant behandelt hat, dabei handele es sich um wenige hundert im Jahr, befinde sich kein E-Mail-Verkehr der Kläger. Auch die Protokollierung dieser Vorgänge würden bereits zum Ende des Folgejahres gelöscht. Zwar sei nicht auszuschließen, dass zunächst E-Mail-Verkehre der Kläger erfasst worden sind. Der damit ggf. verbundene Eingriff in Art. 10 GG lässt sich aber nicht mehr feststellen. Selbst wenn solche E-Mails erfasst worden wären, wären sie wie alle anderen nachrichtendienstlich als irrelevant eingestuften Mails im Einklang mit den Bestimmungen des Artikel 10-Gesetzes und den allgemeinen verfassungsrechtlichen Maßgaben für den Datenschutz unverzüglich und spurenlos gelöscht worden.

Der BND ist zur Löschung solcher E-Mails verpflichtet, weil nach dem gesetzlichen Konzept eine Benachrichtigung der Betroffenen über die Erfassung dieser E-Mail-Verkehre nicht vorgesehen ist. Dies stehe im Einklang mit Art. 10 GG i. V. m. Art. 19 Abs. 4 GG, weil dadurch eine Vertiefung von Grundrechtseingriffen durch Speicherung der Daten einer unübersehbaren Zahl von Grundrechtsträgern vermieden wird. Die damit verbundene Rechtsschutzlücke sei wegen der Gewährleistung kompensatorischen Grundrechtsschutzes durch die G10-Kommission hinnehmbar.

Die Klagen mit dem Ziel, eine Speicherung und Nutzung von Metadaten in dem System VERAS zu unterlassen, beurteilte das BVerwG als noch nicht entscheidungsreif. Die in VERAS gespeicherten Metadaten nutzt der BND zur Erstellung von Verbindungsanalysen. Nach Angaben des Dienstes werden die Metadaten aus dem deutschen Telefonverkehr „anonymisiert“ gespeichert. Das bedeute, dass die Telefonnummer, IMEI und ISIM ab der sechsten Stelle gelöscht würden, alle anderen Daten wie die Funkzelle, die Zeiten des Beginns und Ende der Kommunikation und dergleichen bleiben erhalten. Dieses Vorgehen des BND bedürfe weiterer gerichtlicher Aufklärung. Für Prozessbeobachter zeichnet sich ab, dass das Gericht im weiteren Verfahrensgang durch Sachverständige begutachten lassen wird, inwieweit die in VerAS gespeicherten Daten auch bei anonymisierter Telefonnummer aufgrund weiterer Informationen einer Person zugeordnet werden können. Als möglicher Gutachter war die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) Andrea Voßhoff im Gespräch. Das Gericht wird dem BND aber auch Gelegenheit geben, seinen Vergleichsvorschlag zu prüfen: Dazu soll der Geheimdienst die Kläger in einer Art Whitelist von der Speicherung in VerAS ausschließen. Ob dies möglich und sinnvoll sei, konnten die Vertreter der Behörde vor Ort nicht beantworten und erbaten sich eine Bedenkzeit (BVerwG, PM 15.12.2016 Nr. 105/16, Klage gegen BND wegen strategischer Überwachung von E-Mail-Verkehr in den Jahren 2012 und 2013 erfolglos; weiterer Aufklärungsbedarf wegen einer Speicherung und Nutzung von Daten im System VERAS; Gerber, Bundesverwaltungsgericht lehnt Klagen gegen BND teilweise ab, www.heise.de 15.12.2016).

BAG

Mitbestimmungspflicht bei Facebook-Auftritt mit Posting-Funktion

Das Bundesarbeitsgericht (BAG) in Erfurt entschied mit Beschluss vom 13.12.2016, dass die Ausgestaltung einer Facebook-Seite, mit der ein Arbeitgeber Facebook-Nutzenden die Veröffentlichung von sogenannten Besucher-Beiträgen (Postings) ermöglicht, die sich nach ihrem Inhalt auf das Verhalten oder die Leistung einzelner Beschäftigter beziehen, der Mitbestimmung des Betriebsrats unterliegt (1 ABR 7/15).

Beklagter Konzern und Arbeitgeberin in dem Verfahren war der DRK-Blutspendedienst West in Hagen. Bei den Blutspendeterminen sind ein oder mehrere Ärzte sowie bis zu sieben weitere Beschäftigte tätig. Sie tragen Namensschilder. Im April 2013 richtete die Arbeitgeberin bei Facebook eine Seite für konzernweites Marketing ein. Bei Facebook registrierte Nutzer können dort Postings einstellen. Nachdem sich Nutzende darin zum Verhalten von Beschäftigten geäußert hatten, machte der Konzernbetriebsrat geltend, die Einrichtung und der Betrieb der Facebook-Seite sei mitbestimmungspflichtig. Die Arbeitgeberin könne mit von Facebook bereitgestellten Auswertungsmöglichkeiten die Beschäftigten überwachen. Unabhängig davon könnten sich Nutzende durch Postings zum Verhalten oder der Leistung von Arbeitnehmern öffentlich äußern. Das erzeuge einen erheblichen Überwachungsdruck.

Die Rechtsbeschwerde des Betriebsrats gegen die Abweisung seiner Anträge durch das Landesarbeitsgericht Düsseldorf am 12.01.2015 (9 TaBV 51/14) hatte vor dem Ersten Senat des BAG teilweise Erfolg. Der Facebook-Auftritt alleine schade den Beschäftigten nicht. Der Mitbestimmung unterliege aber die Entscheidung der Arbeitgeberin, Postings unmittelbar zu veröffentlichen. Soweit sich diese auf das Verhalten oder die Leistung von Arbeitnehmern beziehen, führt das zu einer Überwachung von Arbeitnehmern durch eine technische Einrichtung im Sinne des § 87 Abs. 1 Nr. 6 BetrVG (Mitbestimmung des Betriebsrats beim Facebook-Auftritt des Arbeitgebers, BAG PM 13.12.2016; Bundesarbeitsgericht: Betriebsrat darf bei Facebook-Auftritt mitreden, www.heise.de 13.12.2016).

Niedersächsisches OVG

Speicherung gewaltbereiter Fußballfans weitgehend zulässig

Das Niedersächsische Oberverwaltungsgericht (OVG) in Lüneburg ent-

schied mit Urteil vom 18.11.2016, dass die Polizei prinzipiell die Daten gewaltbereiter Fußballfans speichern darf (Az.: 11 LC 148/15). Mit der Klage gegen die Polizeidirektion Hannover erzielte ein weiblicher Fußballfan damit nur einen kleinen Teilerfolg. Die Frau hatte die Löschung von allen Einträgen über sich verlangt, gelöscht werden soll jedoch gemäß der Entscheidung nur einer. In der Berufungsverhandlung hatte die Klägerin mehrere Zeugenbeweisanträge zu einzelnen Einträgen in der Datei gestellt. Der 11. Senat hatte einem Zeugenbeweisantrag stattgegeben, der sich auf einen Eintrag bezieht, in dem eine Gefährderansprache am 12.07.2014 vermerkt ist. Die Klägerin stellt unter Benennung von Zeugen unter Beweis, dass an diesem Tag ihr gegenüber eine Gefährderansprache nicht durchgeführt worden ist. Das OVG urteilte darüber aber ansonsten, dass die Einträge für die Erfüllung der Aufgaben der Polizei, Gefahren abzuwehren und Straftaten zu verhindern, weiterhin erforderlich seien: „Nach Ansicht des Gerichts wird die Arbeitsdatei unter Beachtung datenschutzrechtlicher Vorgaben geführt". Eine Revision ließ das Gericht nicht zu.

In dem Verfahren ging es um sogenannte SKB-Dateien der Polizei (Arbeitsdatei Szenekundige Beamte), die sich in der Fanszene auskennen. Solche Dateien werden von der Polizei in Hannover, Braunschweig und Wolfsburg geführt. Dort sind nach Polizeiangaben derzeit rund 1200 Menschen aufgelistet. Gemäß einem Sprecher der Polizeidirektion Braunschweig liegt die Erfassung bei den zuständigen Dienststellen in Städten mit Vereinen aus der ersten, zweiten und dritten Fußballbundesliga. Dort seien rund 250 Menschen erfasst, in Wolfsburg etwa 200. Die szenekundigen BeamtInnen sollen alle Delikte rund um die Fußballspiele bearbeiten. Auch in der Prävention werden sie eingesetzt, etwa bei der Erstellung von Gefahrenprognosen vor Spielen. Auch mit den Fans stünden die BeamtInnen dabei in engem Kontakt. Gemäß einem Sprecher der Polizeidirektion Hannover verfügt jeder Standort über eine eigene Datensammlung. In Hannover seien rund 750 Menschen erfasst.

Das Verwaltungsgericht (VG) Hannover hatte am 26.03.2015 die Datenspeicherung in erster Instanz im März 2015 für grundsätzlich zulässig erklärt und die Klage der Frau zum überwiegenden Teil abgewiesen (10 9932/14). Nur drei Daten müssten gelöscht werden, entschied das VG damals. Behörden dürften Daten zum Zweck der Gefahrenabwehr erheben und speichern. Die Arbeitsdatei SKB diene auch der Verhütung von Straftaten. Bei strafrechtlichen Ermittlungsverfahren erhobene Daten dürften daher aber nur aufgenommen werden, wenn der Verdacht besteht, dass die oder der Betroffene künftig vergleichbare Straftaten begehen wird (Entscheidung über Anspruch auf Löschung personenbezogener Daten in der „Arbeitsdatei Szenekundige Beamte" vertagt, http://www.oberverwaltungsgericht.niedersachsen.de 25.08.2016; OVG Niedersachsen: Polizei darf Daten gewaltbereiter Fußballfans speichern, www.heise.de 19.11.2016).

Buchbesprechungen



Kühnl, Christina
Persönlichkeitsschutz 2.0 – Profilbildung und -nutzung durch soziale Netzwerke am Beispiel von Facebook im Rechtsvergleich zwischen Deutschland und den USA
De Gruyter Berlin Boston 2016,
99,95 €, 406 S.
ISBN 978-3-11-048562-2

(tw) Die Diskussion über den Datenschutz im Internet hat inzwischen derart viele Facetten, dass einige der ursprünglichen und grundlegenden Aspekte nicht mehr mit der nötigen Aufmerksamkeit besprochen werden. Ein solcher Aspekt ist die Profilbildung, die insbesondere durch soziale Netzwerke erfolgt, von denen das weiterhin weltweit größte Facebook ist. Die unter der Anleitung von Prof. Peifer in Köln entstandene Doktorarbeit von Christina Kühnl hat den Verdienst, die damit auftauchenden rechtlichen Fragen transatlantisch zu behandeln und zu beantworten. Dabei verfolgt sie das äußerst lobenswerte Anliegen, eine möglichst große Schnittmenge zwischen den US und Deutschland bzw. Europa zu finden, um auf dieser Basis einen gemeinsamen regulierten Selbstregelungsansatz – für einen transatlantischen Code of Conduct – zu finden.

Dabei herausgekommen ist eine äußerst umfassende und tiefgehende Analyse des Facebook-Profilings sowie der rechtlichen Antworten in Deutschland und den USA. Dabei behandelt die Autorin in juristisch souveräner und sprachlich gut verständlicher Art sämtliche Aspekte des Profilings, von den technischen über die materiellrechtlichen bis hin zu den prozessualen, z. B. den Zuständigkeits- und Anwendungs-Fragen unter Berücksichtigung aller Ebenen – von der grundrechtlichen über die einfachgesetzliche – einschließlich der Datenschutz-Grundverordnung (DSGVO) – bis hin zur Rechtsprechung und zur Anwendung durch die Aufsicht. Für die deutsche LeserIn besonders aufschlussreich sind dabei einerseits die technische Beschreibung des Profilings durch Facebook sowie die sehr aktuelle, knappe und dennoch umfassende Darstellung des US-Datenschutzrechts

Dabei erweist sich das Anliegen der Autorin, den Datenschutz in den USA und in Deutschland/Europa zusammenzubringen, schon auf rechtlicher Basis als äußerst schwierig. Die Rechtsprechung des US-Supreme Court zur weiten Geltung des First Amendments (Meinungsfreiheit) und zur beschränkten Anwendung des Fourth

Amendmends (Schutz vor Durchsuchung, reasonable expectations of privacy) lässt sich nur – und das nur begrenzt – nach Europa transferieren, wenn die kritische Literatur und Minderheitenpositionen im Supreme Court (z. B. Sotomayor in der U.S. v. Jones-Entscheidung) zur Grundlage genommen werden. Betrachtet man dagegen die Gesetzeslage, die herrschende Rechtsprechung sowie die Praxis, insbesondere auch der Federal Trade Commission (FTC), dann könnte man verzweifeln. Doch das tut die Autorin nicht, sondern reiht die relevanten Informationen aneinander, um eine möglichst faktenbasierte Einschätzung zu ermöglichen.

Die Doktorarbeit wurde im November 2015 angenommen; die vorliegende Textfassung berücksichtigt Änderungen bis Mai 2016. Dies zwang die Autorin, nachträglich die Safe-Harbor-Entscheidung von Oktober 2015, die DSGVO und das Privacy Shield einzuarbeiten. Dies erfolgte bruchfrei, wenngleich dabei die Relevanz dieser rechtlichen Umstände nicht hinreichend gewürdigt werden konnte und die Bewertung des Privacy Shield allzu optimistisch ausfällt. Auch mag der Rezensent nicht alle dargelegten Positionen teilen, die aber (damals) sämtlich der in Deutschland herrschenden Meinung entsprachen, etwa wenn bei der Frage zur Verantwortlichkeit die gezielte Arbeitsteilung zwischen Fanpagebetreibern und Facebook nicht gesehen wird, zu stark an die tatsächliche Datenverarbeitung anknüpft und nicht an die ökonomischen Interessen, wenn der Einwilligung eine zu hohe Legitimationskraft zugesprochen wird oder die Geheimhaltung von Auswertungslogiken durch die Verantwortlichen akzeptiert wird. In jedem Fall wird der Meinungsstand qualifiziert referiert, so dass die Meinungsbildung der LeserIn eine gute Grundlage erhält.

Da es sich bei der Arbeit um eine juristische Dissertation handelt, blendet sie ökonomische und politische Aspekte weitgehend aus. So richtig dies dogmatisch ist, so schwer erschließt sich die faktische Unmöglichkeit des rechtlichen Anliegens der Autorin – den transatlantischen Datenschutz zu versöhnen. Dies ändert nichts an der Richtigkeit des Anliegens und auch nicht daran, dass diese Arbeit hierfür äußerst hilfreich ist. Ob diese Fakten in den postfaktischen Zeiten eines US-Präsidenten Trump noch Wirksamkeit entfalten werden, kann erst die Zukunft erweisen. Das Werk ist für alle, die zum Profiling, zu sozialen Netzwerken und zum transatlantischen Datenschutz arbeiten, eine große wertvolle Hilfe. Insofern hat sie – auch wenn dies nicht ihr primäres Anliegen ist – hohe Relevanz für die praktische Umsetzung der Profiling-Regelung in Art. 22 DSGVO.

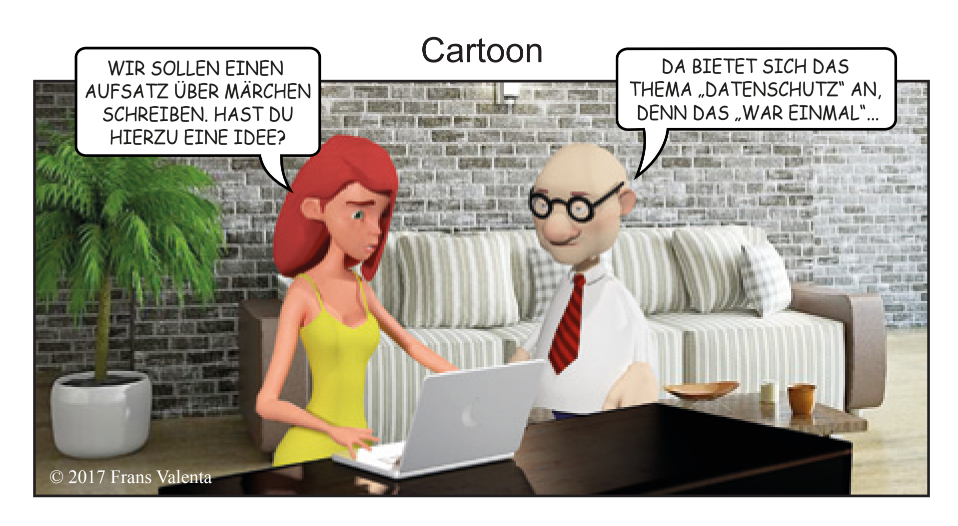


Paal, Boris P./Pauly, Daniel (Hrsg.)
Datenschutz-Grundverordnung
2017, 891 S., ISBN 978 3 406 69570 4, 99,00 €

(tw) Nach einer Vielzahl von systematischen Darstellungen (DANA 2016, 158 f., 206 ff.) liegt nun die erste umfassende, sich ausschließlich der europäischen Datenschutz-Grundverordnung (DSGVO) widmende Kommentierung vom C. H. Beck-Verlag vor. Dabei betreten neue Autoren die Bühne der Datenschutz-Kommentare: Neben den Herausgebern, einer Professor in Freiburg, der andere Anwalt in Frankfurt, haben beigetragen Stefan Ernst, Anwalt aus Freiburg, Eike Michael Frenzel, Dozent in Freiburg und Mario Martini, Professor in Speyer. Barbara Körffer, stellvertretende Landesdatenschutzbeauftragte in Kiel, welche mit dem Hintergrund eigener Praxiserfahrung die Regelungen zur Datenschutzaufsicht und zur Kohärenz bearbeitete, war bisher mit Kommentierungen zum BDSG im Gola/Schomerus vertreten. Doch sind auch die anderen Autoren publizistisch im Datenschutz keine Unbekannten.

Das Ziel des Kompakt-Kommentars war es offensichtlich, schnell, nämlich schon im Oktober 2016, auf den Markt zu kommen, weshalb der Anspruch nicht darin besteht, eine vertiefte Bearbeitung zu bieten; sie soll vielmehr „kurz und bündig“, so die Werbung, sein. Dass hierfür dann doch eine Menge Papier bedruckt werden muss, zeigt, dass die DSGVO eine sperrige Materie ist. Den AutorInnen gelingt es aber, diese so darzustellen, dass sie handhabbar wird, indem die Genese, die Erwägungsgründe und die Regulierung zueinander in Bezug gesetzt werden. Zu kurz kommen zwangsläufig oft praktische Anwendungsfragen, was auch dem wissenschaftlichen Hintergrund der meisten Autoren geschuldet sein dürfte. Während aber die bisherigen systematischen Darstellungen jeweils eine akribische Suche der Rechtsquellen nötig machen, sind diese hier gemäß der Systematik der DSGVO leicht und nachvollziehbar erschlossen. Die Kommentierungen verweisen auf aktuelle Literatur und geben erste Hinweise, die für die Auslegung relevant sind. Dass dabei nicht immer ins Schwarze getroffen wird, etwa bei der Bearbeitung der Geheimnisregelungen, war wohl nicht zu vermeiden. Die Grundgedanken der DSGVO, Literaturhinweise, Verweise auf die Rechtsprechung des EuGH und manche weitere Auslegungshilfe sind zu finden. Insofern ist die Kommentierung eine nützliche Hilfe.

Cartoon



Marktkonformer Datenschutz



Daten als das neue Öl, das neue Gold, als Währung, als Produktionsfaktor, als Rohstoff des 21. Jahrhunderts. Viele – mal mehr, mal weniger gelungene – Bilder wurden in den vergangenen Jahren entworfen, um die Bedeutung von Daten für die digitale Entwicklung zu unterstreichen. Mittlerweile hat wohl jeder verstanden, dass Daten auch zu attraktiven Wirtschaftsgütern geworden sind.

Thomas de Maizière in einem Gastbeitrag des Tagesspiegel vom 16.02.2017
http://www.tagesspiegel.de/politik/data-debates-datenschutz-ist-kein-selbstzweck/19391956.html